EXHIBIT 2

Declaration and Report of

Jeremy Clark PhD.

Declaration of Jeremy Clark

in Support of Motion for Class Certification

Jeremy Clark, Ph.D., P.Eng.

November 13, 2025

Contents

1 Preliminaries

1.1 Assignment

I have been engaged by Plaintiff Trenton Smith ("Plaintiff"), through their counsel, to provide a declaration in the case captioned *Trenton Smith v. John Shahidi*, Case 8:25-cv-161-FWS-DDFM, pending in the United States District Court for the Central District of California – Southern Division. Plaintiff has retained me to independently analyze the Full Send Metacard non-fungible token (henceforth Metacard NFT), its implementation, the mechanisms used to purchase it and establish its price, and the data associated with its purchases and trades; and to opine on issues relating to the class certification of the case.

1.2 Qualifications

I am an associate professor at the Concordia Institute for Information Systems Engineering (CIISE) at Concordia University in Montreal, QC, Canada. From 2019–2025, I held the NSERC/Raymond Chabot Grant Thornton/Catallaxy Industrial Research Chair in Blockchain Technologies. I hold a Ph.D. in Computer Science from the University of Waterloo, awarded

in 2011 with the university's Alumni Gold Medal, and in the discipline of applied cryptography. I am a professional engineer (P.Eng.) with the Professional Engineers of Ontario (PEO).

I have over a decade of research expertise in digital assets and blockchain, and even more experience with related areas of cryptography. My expertise includes material knowledge of Bitcoin and Ethereum.

Bitcoin was described in late 2008 and released as software in early 2009. I began pursuing academic research on Bitcoin in 2011 and have published over 20 peer-reviewed papers on Bitcoin, Ethereum, digital assets, blockchain technology, and similar topics. Research highlights include CommitCoin [2], one of the earliest academic works on Bitcoin published in *Financial Cryptography and Data Security* (Conference Rank:[1] A) in 2012; our 2015 systemization of knowledge on Bitcoin and blockchain research [1] published in *IEEE Symposium on Security and Privacy* (Conference Rank:[2] A+; citations 1000+[3]); and our 2017 article on Bitcoin's academic pedigree [4] published in the *Communications of the ACM* (Journal Impact Factor:[4] 14.065; downloads: 300K+[5]).

I have testified on digital assets to the Standing Senate Committee on Banking, Commerce and Economy of the Senate of Canada (April 3, 2014), and to the Standing Committee on Finance of the House of Commons of Canada (March 27, 2018). I have given over 50 presentations on digital assets to companies, government agencies, law enforcement, pension plans, and academic groups.

My attached CV contains further evidence of my expertise and research impact in these subjects.

[1] CORE Conference portal, Feb. 2024.

[2] CORE Conference portal, Feb. 2024

[3] Google Scholar, Feb. 2024.

[4] Clarivate / Web of Science, Feb. 2024.

[5] 293 530 Queue + 41 257 CACM, ACM Digital Library, Feb. 2024

1.3 Facts, data, and documents relied upon

To prepare this report, I reviewed all legal documents and discovery presented to me by counsel. I reviewed the technical information distributed online about Metacard NFTs, including archived webpages through the Internet Archive's service The Wayback Machine.

My measurements mostly involve blockchain records from the Ethereum blockchain; this includes transactions, function calls, ERC-20/721 logs, and contract bytecode/ABI. I relied upon datasets curated and offered through the tool Dune Analytics; this includes:

- `nft.transfers`,
- `nft.trades`,
- `tokens.transfers`,
- `metacard_ethereum.fullsend_call_`*$function*, and
- `metacard_ethereum.fullsend_evt_`*$event*.

For attributing pseudonymous Ethereum addresses to known identities, I relied on Etherscan and Arkham Intelligence, noting that third-party labeling can be error-prone. For discovering transaction flows, I relied on the tools Arkham Intelligence and Breadcrumbs and their associated datasets. For examining NFT artifacts, such as the image associated with them, I relied on the Interplanetary File System (IPFS) and the service ipfs.io gateway. Finally, as necessary, I also reviewed the technical details of Ethereum from the Ethereum Yellow Paper, Solidity by Example, relevant EIPs/ERCs, and other public documentation.

1.4 Principles and methods

I reviewed the complaint[6] and disclosure provided by Plaintiff's attorneys. I reviewed background information and relied on my past research to understand the technology involved. I

[6]Second Amended Complaint For Damages, 8:25-cv-161-FWS-DDFM, Document 80, Filed 10/07/25. Henceforth "Second amended complaint."

was asked to reconstruct the Metacard mint, rarity assignment, and secondary market sales, and to trace royalty payments and proceeds from the sale. I located the Metacard NFT smart contract address on Ethereum. For the reconstruction, I used the data disclosed in the previous paragraph. I formulated the measurements needed and used the appropriate dataset(s) to reconstruct the data. Using the data, I provide class-wide metrics and determinations that can be made about individual wallet addresses' profits and losses with respect to Metacard NFTs. I provide more specific methodological details in each section below.

1.5 Disclaimers

For serving as an expert witness, I am remunerated by *EKSM, LLP* at $400 USD per hour. My compensation is not dependent upon me reaching any specific conclusion or opinion. All opinions are mine and do not necessarily reflect those of Concordia University or any sponsors of my research grants and chair. I have never purchased or knowingly[7] owned a Metacard NFT. Portions of this report may be copied or adapted from reports I have solely authored in the past.

2 Overview of technology

In this section, I provide an overview of the relevant technology and a summary of cryptocurrencies, Ethereum, non-fungible tokens (NFTs), and secondary marketplaces.

2.1 Blockchain technology

Bitcoin. Described in 2008 and launched in early 2009, the Bitcoin cryptocurrency introduced a digital system for asset creation and transfer that is operated through the consensus, at every step, of a set of independent servers all around the world, with no one server in charge. Bitcoin is designed to run on the internet and since the internet contains hostile enti-

[7]Given the way Ethereum operates, anyone at any time could opt to 'airdrop' tokens to one of my Ethereum addresses without my consent, causing me to own them.

ties, the system is designed to run correctly even when a fraction of the servers are malicious and try to attack the system. We also say that Bitcoin is an "open" and "permissionless" system. Open means that anyone on the internet with the appropriate technical capabilities is invited to join the system. Permissionless means that joining the system (and leaving the system) does not require the authorization of any entity in the system. The protocol itself may impose rules about how and when servers can join but ultimately, a permissionless system will let anyone join eventually if they meet the in-protocol prerequisites. Once operating in the system, the servers (called miners or validators) work on verifying and recording transactions in a data structure called a blockchain, which uses cryptographic techniques to provide data integrity.

Ethereum. After the initial success of Bitcoin, a group of enthusiasts believed that an open and permissionless blockchain could be useful beyond use-cases like the transfer of assets. Bitcoin itself is limited in terms of what it can do beyond this. After failing to convince the Bitcoin community to expand the scope of Bitcoin, they created a competitor called Ethereum. The Ethereum blockchain began producing blocks in July 2015. The key difference of Ethereum is that users can design and deploy custom software applications (called "smart contracts") and have the validators run these applications for them. Smart contracts might allow users to make custom tokens, trade Ethereum's digital asset ETH for these tokens, borrow tokens, invest in tokens, purchase financial derivatives based on tokens, and many other use-cases that are now called "decentralized finance (DeFi)." The most popular smart contracts in addition to DeFi, according to the website DappRadar,[8] allow gambling, gaming, social platforms, and transacting digital art. "Smart contracts" are essentially computer programs or applications. They are sometimes called "decentralized applications" or Dapps instead.

[8] "Top Blockchain Dapps," Dapp Radar, Retrieved Jan–Feb 2025.

Ethereum[9] begins with the same capabilities as Bitcoin: users can create addresses to receive and send ETH, which is Ethereum's on-chain currency. Ethereum is designed with a new kind of transaction where a user can submit the code of a computer application (or a "contract") to Ethereum. The contract will be assigned an address and its code will be stored on the blockchain at this address. The user pays a fee to deploy a contract (proportional to the size of the contract). An address is a long, random sequence such as: `0x7eCb204feD7e386386CAb46a1fcB823ec5067aD5` which we will abbreviate as `0x7e...7aD5`. If the reader clicks on an abbreviated address, it will open a list of the address's activities on the website Etherscan.

At this point, the user who created the contract could disappear, and the application will still live on the blockchain and be accessible to current and future Ethereum users. Contracts are "autonomous" which means they cannot perform computations by themselves ("in the background") the way a computer or smartphone application might. Contracts only run code when users ask Ethereum to run the contract (and pay for it). Once the user-requested computation is completed, the contract code hibernates until the next user requests that it runs. What users are allowed to run computations and what computations a contract can perform are contained in the code of the contract itself (and can be anything the programmer of the contract decides when programming it).

While a sophisticated user might interact with a smart contract directly on Ethereum, most contracts are accompanied by a website with graphics, text input, buttons, and other user interface elements that will interact with Ethereum and the smart contract. A user will navigate to the website and if they wish to use the contract, they will "connect" the website to the Ethereum (or Ethereum-compatible) software they are using to manage their signing keys (called a "wallet"). The website will pass the cost and other details of what the user wants to do (called a "transaction") to the user's wallet software (*e.g.,* MetaMask). The wallet software will display the information to the user and ask the user for consent to

[9]Note that when relevant, this report describes how Ethereum operated during the relevant period (14 May–27 June 2021) and will differ from how it operates today, especially as it pertains to gas fees, consensus, and data storage.

execute the transaction (typically requiring a password) or provide an option to cancel the transaction.

Ethereum fees. To ensure validators are fairly compensated and to combat malicious actors from stalling the network ("denial of service" attacks) by asking for a long-running computation to be performed, all computations are broken into small steps ("instructions" or "opcodes") where each step is assigned a value in a unit called "gas." The value represents how complex the computation step is to execute or store (*e.g.,* a multiplication has a higher gas value than an addition). Users then specify a rate of ETH per unit of gas that they are willing to pay as a fee to the validator who includes their transaction in a block. In practice, the user's software examines the current conditions of Ethereum and suggests a rate to the user. The main takeaways are: (1) all computations cost the user ETH in fees, (2) more complex computations cost more than simpler ones, and (3) validators earn revenue by performing computations on Ethereum.

2.2 Non-Fungible Tokens (NFTs)

Description. One use-case of Ethereum is to create digital assets, record their ownership, and permit transfers of these assets. Anyone on Ethereum can create a collection of 1 or more NFTs in a smart contract. Each token in the collection has a unique identifier (called the token ID) and the contract maintains a mapping of which Ethereum address owns each token ID. The asset itself is not necessarily stored on Ethereum and might be accessible through a pointer to a web address or file storage service, the most common for blockchain applications being the InterPlanetary File System (IPFS).

At the time of writing, uses of NFT collections include collectibles (trading/sports cards), digital artwork, membership passes, video game items (character skins and in-game items) and credentials (tickets, certificates, and records).

By operating on Ethereum, NFT collections tend to exhibit a high degree of permissionlessness over their operations. Anyone can create an NFT collection and Ethereum will

maintain the system in perpetuity. Owners of NFTs can transfer ownership at any time without permission.

The Ethereum community has developed standards for NFT collection contract code, including reference implementations. The minimal, widely adopted standard is called 'ERC-721: the non-fungible token interface' and a reference implementation of ERC-721 is provided by the software company OpenZeppelin. The Metacard NFT adapts v4.4.1 of this software. The importance of using a standards-compliant implementation is that other Ethereum contracts and websites already know how to trigger actions in the NFT contract, even if they were written before the NFT collection was released. This allows interoperability between the NFT collection and many existing services for trading and displaying NFTs.

Secondary markets. Several companies, including OpenSea and LooksRare, operate public NFT marketplaces which find and index ERC-721 (and other standard) NFTs once they are created on Ethereum. Users can use these platforms to trade NFTs with other users, using cryptocurrencies like ETH (or an interoperable variant of ETH called WETH) or stablecoins like USDC. The sites often offer credit card services, typically with an external payments processor (*e.g.,* MoonPay) that will purchase the requisite cryptocurrency and complete the transaction.

Standards-compliant NFTs can be listed and traded on secondary markets without the explicit permission of the owner of the NFT collection. However on OpenSea and LooksRare, the owner can 'claim' the NFT by proving ownership over the NFT collection's smart contract. This allows the owner to customize and brand the landing page for the collection. By registering, the owner can also deploy a royalty (optional or mandatory) on every sale of an NFT from the collection made through the website.

3 Reconstructions

3.1 Metacard Mint

This case involves the NFT called Full Send Metacard (henceforth Metacard). I was asked to reconstruct the minting process. I used Etherscan to obtain a copy of the smart contract code. I examined the code and chronology of early blockchain activities using Etherscan. I examined archives of websites affiliated with the NFT with the Internet Archive. Once I identified the function calls for minting NFTs, I used Dune Analytics to find data about each minting activity. On Dune, I used the decoded projects data `metacard_ethereum.fullsend_call_`*$function* where *$function* is a placeholder for a function name like `mint` or `mintfriendsfamily`. Similarly I relied on `metacard_ethereum.fullsend_evt_`*$event*. From this dataset, I obtained the data I will present below.

When an NFT collection is launched, the NFTs need to be created and assigned to their first owners. Minting is the Ethereum-based activity of creating the new token ID and assigning it to the owner's address. For some NFTs, the owner of the collection will allocate the NFTs to owners. For other NFTs, including Metacard, users who want to own an NFT will initiate the minting process by interacting with the contract. Typically a user will do this through a software client, such as a wallet like MetaMask. In this case, they will visit the website `https://fullsend.metacard.io`, connect their wallet, and follow the website prompts to mint an NFT.

The code for the Metacard NFT collection was deployed on Ethereum and finalized on 19 Jan 2022 at 10h19m UTC. It was given the address `0x7e...7aD5`, which I have abbreviated for readability, however clicking the address in this report's PDF file will provide the full address and its description on Etherscan. The address of the entity that created the NFT collection is `0x9E...C731`. The code of the Metacard NFT appears to be an adaptation of a standard NFT library from OpenZeppelin at version 4.4.1. I noted that the code was modified to enable early rounds of minting that would be limited to, what the code calls, 'friends and family' and to a 'whitelist' before allowing any user on Ethereum to mint NFTs.

Figure 1: Website describes a 'whitelist pre-sale' with no mention of the earlier internal sale or the earlier friends and family sale. Note the times say 9:30 am and 12:30 pm despite the font making them appear like 9:38 am and 12:38 pm (users who misinterpreted the time would have arrived too late to participate in the first sale and would have only caught the final minute of the second).

The collection includes 10000 NFTs numbered from 1 to 10000. During the mint, the price of one NFT was set to 0.75 ETH. The number of NFTs that could be minted by a single address was limited to 10.

The first 101 NFTs were minted on 19 Jan 2022 at 14h54m UTC (6:54am PST) by the address that created the NFT contract `0x9E...C731`. Although purchases were limited to 10 NFTs per address, because this address had administrative rights within the NFT contract, it was able to mint as many NFTs as it wanted for free.

The next 399 NFTs were earmarked for what the code called a 'friends and family' sale that began at 16h02m UTC and sold out 12 minutes later at 16h14m.

The next 3000 NFTs were earmarked for what the code called a 'whitelist' sale and the Metacard website called at 'whitelist presale.' The website did not disclose either of the two earlier sales (see Figure 1). The sale began at 17h30m UTC and sold out by 17h34m UTC.

The final 6500 NFTs were earmarked for a public sale. The sale opened at 20h29m UTC and sold out at 20h38m UTC.

Each Ethereum address could purchase between 1 and 10 NFTs. The number of unique addresses purchasing at least 1 NFT is shown in Figure 2a for each stage of the minting process. Figure 2b shows how many addresses made only 1 purchase, made 2 purchases, *etc.*. The 10000 NFTs were purchased by 5226 unique addresses. Most addresses (3404) bought the smallest amount of 1 NFT, while 161 addresses bought 10 NFTs. At least one address appears to have used a 'bot' to generate temporary addresses that could purchase 10 NFTs each and was able to complete 4 purchases of 10 NFTs for a total of 40 NFTs.

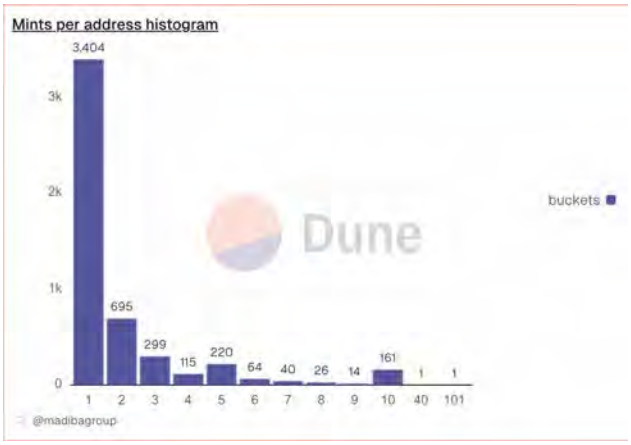
Query results Mints per phase

phase	tokensMinted	uniqueAddresses	firstBlock	lastBlock
internal	101	1	14036611	14036611
friends	399	94	14036917	14036969
allowlist	3000	900	14037327	14037347
public	6500	4231	14038122	14038164

4 rows Search ...

@madibagroup

(a)



(b)

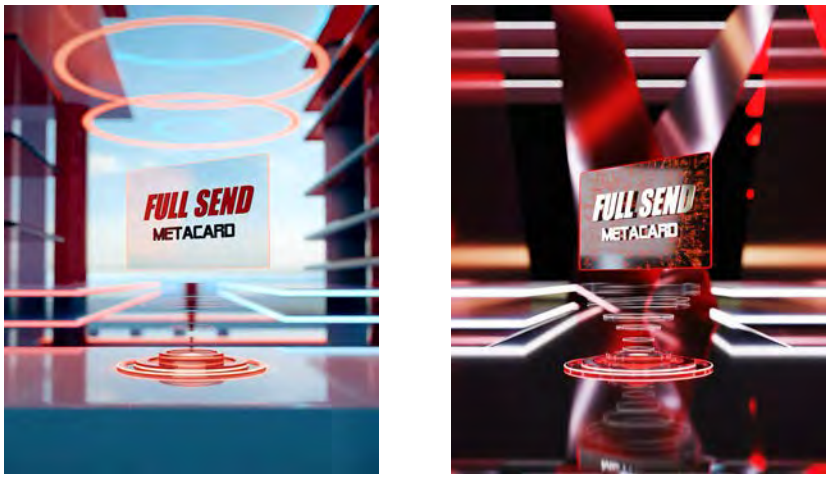
Figure 2: Breakdown of the four stages of the mint, including (a) how NFTs were minted in each stage; (a) how many unique addresses minted an NFT (since an address could mint between 1 and 10 NFTs); and (b) how many addresses purchased between 1 and 10 NFTs, plus two outlier purchases of 40 and 101 NFTs (see text).

Finally the contract that created the Metacard NFT minted the first 101 NFTs.

3.2 Rarity Assignment

I was asked to reconstruct the allocation of common NFTs and rare NFTs amongst the 10000 sold NFTs. To accomplish this, I used Dune Analytics to isolate the function call `Set Base URI` and I used Etherscan to obtain the link to the metadata about the NFT collection on IPFS. I used the software tool IPFS Desktop to obtain the data for each NFT and I used Mathematica to determine the distribution of rare NFTs amongst the 4 minting phases.

The Metacard NFT references an animated image (in the file format of a MP4 digital video) of a spinning card that says 'FULL SEND METACARD' (see Figure 3). A rare version (250 out of 10000) described in the code as 'METACARD CYBER RED' is also available. I will describe these, respectively, as the 'common' and 'rare' variant of Metacard. In the documents I reviewed, I do not recall the rare variant having an additional perks. However, generally, rare NFTs may be considered more collectible and trade at a premium



(a) Common Variant (b) Rare Variant

Figure 3: One frame of the animated image associated with the Metacard NFT

Phase	Total NFTs	Rare NFTs	Percentage Rare
Internal	101	3	2.97%
Friends/Family	399	12	3.01%
Presale Allowlist	3000	66	2.20%
Public Sale	6500	169	2.60%

Table 1: The four phases of the mint and how many NFTs minted in each stage were assigned a rare variant. Baseline rate of rare variants is 2.5%.

price on secondary markets, such as OpenSea which prominently display the rarity of the NFT and allow NFTs to be sorted by rarity.

As mentioned above, the minting process proceeded in four stages: internal mint, friends and family sale, allowlist presale, and public sale. During the minting process, all NFTs were of the common variety when displayed. The next day, on 20 Jan 2022 at 00h59m UTC, the administrator of the Metacard NFT pushed an update to collection that changed the images of 250 selected NFTs into the rare variety. The selection process for how these 250 were chosen was not disclosed to my knowledge. The distribution of rare NFTs amongst the 4 stages of the mint are provided in Table 1. As a percentage, friends and family mints

received the most NFTs.

The NFTs also contained a textual description of the NFT. Prior to revealing the rarity of the NFTs, the description read:

> THE FULL SEND METACARD WILL GIVE EXCLUSIVE ACCESS TO WHAT FULL SEND DOES IN THE PHYSICAL AND METAVERSE. OWNING A FULL SEND METACARD ALLOWS YOU TO GET IN EARLY ON THE WHAT IS THE BEGINNING OF A LONG JOURNEY FOR THE FULL SEND BRAND.

After the rarity reveal, the description for all NFTs was updated to:

> Explore FULL SEND METACARD.
>
> Built on the Ethereum blockchain with a limited supply of 10,000 NFTs, the FULL SEND METACARD will give exclusive access to what FULL SEND does in the physical world and metaverse.
>
> As a company, the FULL SEND goal is to launch more FULL SEND branded ventures, which include lounges, gyms, festivals, casinos, restaurants and more. FULL SEND is going international.
>
> In addition, we will take these same ventures of products and physical locations and will launch them in the metaverse. This will include FULL SEND apparel, virtual stores, virtual festivals, metaverse casinos, and FULL SEND NFT recording artists. This list will continue to grow.
>
> Owning a FULL SEND METACARD allows you to get in early on what is the beginning of a long journey for the FULL SEND brand.

On 4 July 2024, the description was changed again to read:

> FULL SEND METACARD.

3.3 Proceeds from the Mint

I was asked to reconstruct from blockchain records the outflow of the proceeds of the NFT sale. To do this, I used the `tokens.transfers` dataset from Dune Analytics to track ETH and WETH. To help visualize the flow of payments across entities and obtain historical prices of ETH, I also relied on tracing tools BreadCrumbs and Arkham Intel Tracer.

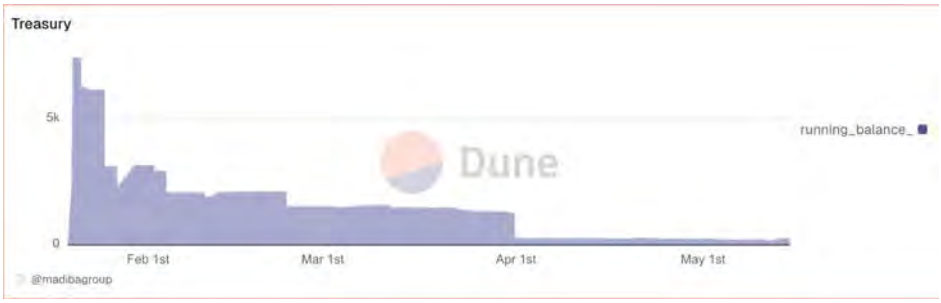


Figure 4: The running balance of the treasury account `0x9E...C731` in ETH from the mint on 19 Jan 2022 to 1 June 2022.

Aside from the 101 NFTs minted during the internal sale, each NFT sale raised 0.75 ETH per NFT for a total of 7424.25 ETH which was worth around $23M USD at the time of the sale. After the initial 3 phases of the mint (internal, friends and family, and presale allowlist) and before the final phase (public sale), the wallet that deployed the NFT collection, `0x9E...C731`, withdrew the 2549.25 ETH raised by the initial sales. Then the public sale began and around 40 minutes later, the 4875 ETH raised in the public sale was withdrawn, again to the same address `0x9E...C731`. Henceforth we will refer to this address as the Metacard treasury.

The treasury address `0x9E...C731` began distributing funds to dozens of addresses over the course of several months. By April 2022, the running balance of the account had been mostly depleted (see Figure 4). The largest net outflow was about 4000 ETH to the address `0x43...2C58` (see Table 2). 31 addresses received a net amount of at least 10 ETH (approximately $28K on 22 Jan 2022 although payments were made over time). If a recipient is known, according to the dataset provided by Arkham Intel, it is labeled in Table 2. If an address is unknown, we determine the address that first sent ETH to it, called the funding address. If the funding address is labeled, we denote it in braces—*e.g.,* (Treasury) means the address had never received ETH until it was first sent by the Treasury address. We apply this with one level of recursion, so ((Treasury)) means an address is unknown, its funding address is also unknown, but the funding address of the funding address was the Treasury.

I also conducted further tracing stemming out from the `0x9E...C731` treasury and as-

Counterparty	Recipient	Net Flow (ETH)
0x430e7b8e07ffda49a4f150d20141e0a802d92c58	(Treasury)	-3992.0839
0x95a36dc32124063477a42c2fc993c9172a8ce71c	(Treasury)	-779.8636
0x267b434428082a685db3337e1b7da2a81084804f	(Treasury)	-711.1575
0xf829d374be3a3d2187de3029d4d21c5913aecc6b	(Treasury)	-549.13
0x51771fa00128ef95579b31b2ba780fe35f0fa108	(Treasury)	-530
0xa62c9f34d0bc5d06370c6dddc320d35fdce472b2	BrennanKarem @ OpenSea	-401.421
0x05e8a5969465fd450961429c7c966f3a1c24edd4	FTX US Deposit	-313.47831
0x0abf9e6a8457cef483694306c03402e8e43400e4	(Treasury)	-258.81
0xa63986cd94aa2df0db430e50c938e2f4795e153d	samshahidi2 @ OpenSea	-159.7396
0x8c87d13fb36ddfa8aebf14a2eb91a3aaf63e6046	(Treasury)	-147.77
0x9cee20365ce2d51b97a661f7ab141baf670e6532	nelkboys @ OpenSea	-146.9946
0xd3ed28c1a29d93aca56b9e3b5f8381418b364d62	Stake.com Deposit	-141
0xaa1d2aebd7503da5d52975aa518f8a4dd24a78c0	((Treasury))	-138.4
0x9bfa964a7ae2b808c7f72af5abf24a17bcfd6969	NFLAgent @ OpenSea	-104.6244
0x9fa402b75b2b0838a5b9569be29c4f864f542dc7	(Treasury)	-97.9559
0xaeb9ab5dd15a8a797bad4ba0067686712c53ec2a	kingkongwilldoit @ OpenSea	-97
0x0032ef315fa10f71a42e8c6917264cca6456eb09	(Treasury)	-87.5314
0x3881942cd11538cfb7d07b96f54b167ff0525199	Gemini Deposit	-75.2967
0x486b2ea071411074f32ba70495038413eb520e40	boredjerky @ OpenSea	-70.78984110391410
0x1b8e6d5ee134f8c7fac3666ab6c8f4fbcc794892	(Treasury)	-66.09
0x80558227e0ff3df973ca2421b57d2f067cb7e8d8	Coinbase Deposit	-64.9
0x594e31691dd0cdc3412bf780ec88c064d7f34aa7	Stake.com Deposit	-63
0x535dd22c0488612500508a7683ebd1b938150726	Nexo Deposit	-55.3338
0xfb130972ce5205e2e0e899298be4b45baf64aefa	(Treasury)	-34.70252134
0x7be8076f4ea4a4ad08075c2508e481d6c946d12b	Ceffu Deposit	-32.9504
0x12d84f05684a2d226351da0883a1b936e7f9c3e5	Coinbase Deposit	-30.6148
0x3a0f3cb627cde38cd127d9416dd85e4194bee0e5	(NeelTPT @ OpenSea)	-27.3069
0xe2c95509c767ba35afca45675f69781184de7499	podcasting @ OpenSea	-23.9632
0x7caaa2ec951dfe07ae25aa71b503ed35dbdc348d	Saliimthedream @ OpenSea	-21.09
0xbb6bce4082f87e8531b4adfb0140b245a6a34883	(Treasury)	-16.0818
0x348ee8db6fdd575fc52114e33286392b4dfa69f6	((Yearn.Finance))	-16.026
0x1804fc5ab929906ee79d013a6f9d279379888e24	(KingSwot @ OpenSea)	-12.44

Table 2: Recipient addresses of net outflows greater than 10 ETH from the Metacard Treasury. If the recipient address is unknown but the first time it received ETH, it was from 'entity,' it is denoted (entity) in braces.

sociated addresses. I noted the plaintiff interrogatory number 8 requests: 'Identify all bank accounts, cryptocurrency wallets, or other financial accounts that held the proceeds from Metacard NFT sales or were used to transact Metacard-related finances.' This would include the addresses in Table 2, as well as addresses downstream from them.

One recipient of to receive proceeds from the Metacard treasury is Stake.com, which maintains multiple deposit wallets for accepting ETH deposits. Stake.com is an online casino and sportsbook that allows gambling with cryptocurrencies including ETH. The treasury directly deposited 141 ETH, plus an additional 63 ETH to Stake.com deposit addresses, as shown in Table 2). The treasury also sent funds to `0x95...e71c` (the second largest recipient

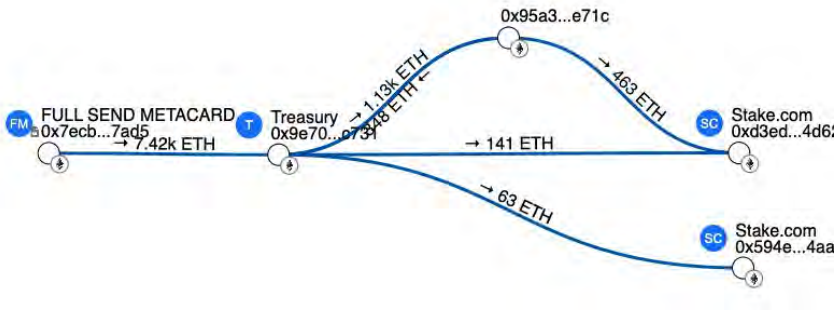


Figure 5: Flows from the Metacard treasury to gambling service Stake.com in USD.

in Table 2) and this address sent 463 ETH to Stake.com (see Figure 5).

3.4 Secondary Market Sales

In order to reconstruct sales of the Metacard NFT on secondary markets, I employed the `nft.trades` dataset from Dune Analytics. Although secondary markets tend to run on third party websites, these websites log the sale of an NFT, including information about the buyer, seller, and price, on Ethereum in a record called an event. The transaction also moves the ETH (or its standards-compliant variant WETH) and NFT between the accounts. The dataset covers OpenSea (15088 sales), Blur (1582 sales), LooksRare (179 sales), and X2Y2 (52 sales). OpenSea and LooksRare were operational at the time of the Metacard mint, while X2Y2 and Blur launched later in 2022. The data presented is updated as to the time of writing (Nov 2025).

Given NFTs follow standardized interfaces, of which the Metacard NFT does, marketplaces automatically discover the NFT without any registration necessary from the owner of the NFT collection. Users began trading the Metacard NFT on the most prominent NFT secondary markets (at the time), OpenSea and LooksRare, before the public minting even started (first trades were made at 16h12m and 17h42m on 19 Jan 2022 respectively). Figure 6 shows the volume and median price over time (the data does not distinguish between common and rare varieties). In January 2022 (the tail-end as the mint happened on 19 Jan),

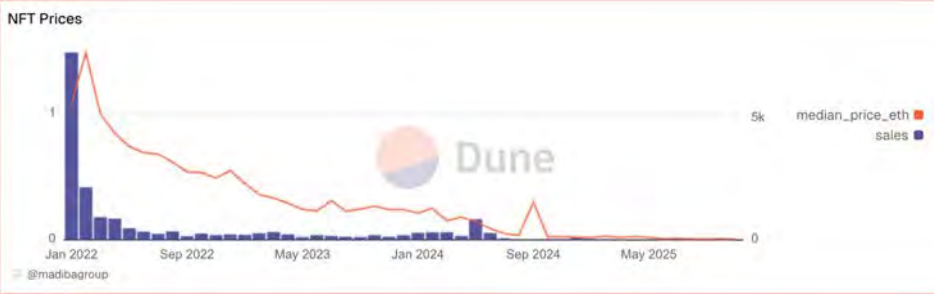


Figure 6: Secondary market sales of the Metacard NFT on marketplaces including OpenSea and LooksRare. Graph depicts number of sales per month and median price (in ETH) per month.

7727 secondary market sales were made at a median price of 1.08 ETH. In February, the sales fell to 2168 while the price rose to 1.47 ETH. By May, sales were 486 and the price was 0.74 ETH which is below the initial minting price of 0.75 ETH. The prices and sales volume have decreased over time.

3.5 Royalties

I was asked to reconstruct royalty payments made to the Metacard addresses as a second source of proceeds from the Metacard NFT. Royalties are made when a Metacard NFT is traded on a secondary market. Royalties are enforced by the marketplace, not by Ethereum or the smart contracts governing the NFT. Thus two traders who arrange an over the counter exchange will not pay a royalty. I first examined the secondary sales using `nft.trades` on Dune Analytics. I determined that only two secondary markets, OpenSea and LooksRare, had a material amount of trading activity.

On the day of the mint, a 10% royalty (called creator earnings) was engaged on the secondary market OpenSea after the friends and family sale and prior to the allowlist presale. Later in the day, after the public minting, a 10% royalty was also engaged on the secondary market LooksRare. The majority of secondary sales, however, were on OpenSea. OpenSea royalties were paid into the `0x9E...C731` and at least 1500 ETH ($4.3M USD at 19 Jan 2022 prices).

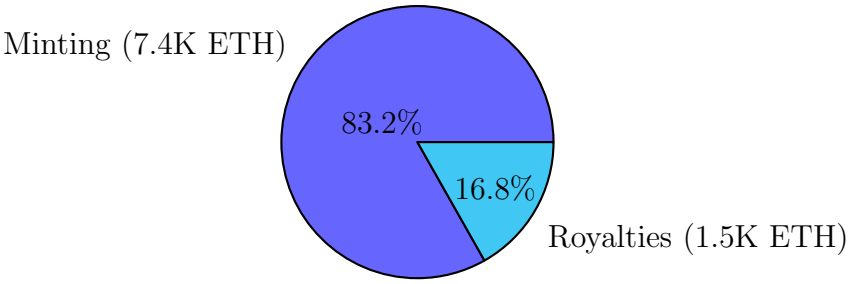


Figure 7: Proceeds from the Metacard NFT including the initial sale and royalties earned on secondary market sales.

3.6 Refunds

The plaintiff complaint describes a refund (or token rescission) program offered for redeeming Metacard NFTs for a undetermined amount of USD, capped at $2300 USD (seemingly plus 7% APY interest).[10] I was asked to reconstruct the refund process from blockchain records however the software platform for redeeming the NFTs is not accessible. Using `nft.transfers` dataset on Dune Analytics, I can determine that over the time-period of the refund program (20 May 2024 to 20 June 2024), two Ethereum addresses received a high volume of NFTs: `0x50...7BEE` and `0xF6...48d0`. At the time of writing, these addresses hold 2594 (26%) and 1287 (13%) of Metacard NFTs respectively. Included in these numbers are most of the 101 tokens from the internal phase of the minting, which were sent to `0x50...7BEE`. Since the refund program was offered alongside an investment opportunity, I would infer that one address was used for those enrolling in the program and the other for those requesting a refund—however I do not know which is which. Neither address returned ETH to the individuals submitting NFTs to these addresses, which coheres with the view that refunds were processed through the US banking system in USD rather than being in blockchain records.

6119 (61%) of metacards were not sent to either address and are thus, presumedly, held by non-participants in the offered programs.

[10] Second amended complaint, ¶112.

4 Opinions in Support of Class Certification

4.1 Opinion 1: The proposed class likely contains thousands of individuals

The plaintiff complaint proposes the class as: "All persons who purchased Metacards through the date of class certification"[11]. It further asserts, "Class Members are numerous that joinder of all of them in a single proceeding is impracticable"[12].

Based on the `nft.transfers` dataset from Dune Analytics, 16,744 unique Ethereum addresses held a Metacard at some point. However one individual may own and operate as many Ethereum addresses as they choose, so the number of individuals could be less than the number of unique Ethereum addresses.

Beginning with the question of how many addresses are operated by a single user, several factors suggest that estimates of the number of addresses per user are likely close to one. In January 2022, the most popular wallet on Ethereum was MetaMask.[13] Coinbase Wallet was also popular[14]. The wallet software for both, by default, creates a single address.

Although operating multiple addresses is possible, it requires the user to take deliberate steps to add more than one wallet. Users may have multiple devices (*e.g.,* a computer and a phone) which may result in having a wallet address on each device. However, activating, using, and maintaining multiple wallet addresses is typically limited to advanced users seeking greater anonymity or untraceability.

One exception may be during the minting phase of the Metacard NFT where the NFT contract limited each unique address to purchasing at most 10 NFTs. According to the complaint, "NFT rarity was assigned at random and was not revealed until after purchase,

[11] Second amended complaint, ¶142.

[12] Second amended complaint, ¶145.

[13] "Consensys Raises $450M Series D Funding as Leading Self-Custodial Wallet MetaMask Reaches Over 30 Million MAUs," 15 March 2022, Online.

[14] 7.4 million monthly transacting users for Q3 2021 from "Coinbase Shareholder Letter Q3 2021," backlinko, Online.

presumably to entice purchases to buy as many NFTs as possible to increase the chance of obtaining an extremely rare NFT." In fact, as described in Section 3.1, at least one apparent individual was able to evade this guardrail and mint 40 NFTs using temporary addresses. Assuming an individual were using multiple addresses to mint more than 10 NFTs, it is reasonable they would try to mint the maximum number of NFTs (10) in each unique address they operated before trying to mint more from a fresh address. We can therefore simply exclude all unique addresses that minted 10 NFTs as possible duplicate individuals. This however is immaterial as only 161 addresses minted the maximum amount (see Figure 2b). Note that once the mint phase was completed, there is no restriction on how many NFTs can be purchased on the secondary market or transferred to a unique address.

If the same user operates more than one address, it is difficult for users to maintain perfect separation of all blockchain activities. Often the user might transfer funds from one address to another, such as consolidating tokens or replenishing addresses running low on ETH, required to pay blockchain fees. These linking activities leave fingerprints in the blockchain that suggest that multiple addresses belong to the same user. For many years, computer scientists have proposed and evaluated algorithms for clustering Ethereum (and other blockchain) addresses together. One project from the Distributed Computing Group at ETH Zürich in 2022 applied clustering heuristics to approximately 7 million Ethereum addresses and determined that the median entity operates 3 unique addresses, with a mean of 4.81 [3].

Beginning with $16,744$ unique Ethereum addresses holding a Metacard NFT and removing the 161 addresses that minted 10 NFTs, we can use the clustering results to estimate that the number of unique Metacard holders are in the range 3448–5528 (the lower bound uses the the mean of 4.81 and the upper bound uses the median of 3).

4.2 Opinion 2: Revenues from the NFT program can be identified from blockchain records and did not stop with the mint

The complaint seeks, "Pursuant to Cal. Civ. Code § 1782(d), Plaintiff and the Class Members seek a Court order enjoining the above-described wrongful acts and practices of Defendants and for restitution and disgorgement"[15] and later seeks, "For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained because of Defendants' wrongful conduct."

Within the proposed class members, some class members purchased at least one Metacard NFT from the initial mint for 0.75 ETH each, which was transferred into the defendants' custody. Other class members purchased NFTs from secondary markets. For these markets, the defendants set a 10% mandatory royalty rate to be remitted to an Ethereum address of their choosing. Thus with each such sale, sellers have a direct economic link with the defendants through this on-going revenue stream, independent of whether they participated in the initial mint.

Blockchain records quantify 7.4K ETH raised at mint and 1.5K ETH later through marketplace royalties, both traced to Ethereum addresses belonging to the project. Revenues include, but are not limited to, both of these amounts.

4.3 Opinion 3: Most class members bought under uniform purchasing mechanics

The complaint asserts that, "Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members"[16]. The reconstructions given in this report support this assertion in terms of the purchasing process. Most class members either bought one or more Metacard NFTs at mint, which was held on the same day at a fixed priced, or they bought on a secondary marketplace. The secondary marketplaces were mainly OpenSea, LooksRare, Blur, or X2Y2 which offer the same core

[15] Second amended complaint, ¶184.

[16] Second amended complaint, ¶146.

functionality of a bid/ask market system.

4.4 Opinion 4: Profits and losses can be established for most class members from blockchain records

For class members that purchased Metacard NFTs during the initial mint and/or traded on NFTs secondary marketplaces, a common and reproducible methodology can apply to all such class members to establish their profits and losses from owning Metacard NFTs without requiring individualized testimony. Provided with a class member's Ethereum address(es), time-stamped blockchain records can establish the purchase and/or sale prices (generally in ETH, convertible to USD using daily exchange rates) for each held NFT to establish a total profit or loss. Any unsold NFTs can be assigned zero or *de minimis* value. Standardized rules (*e.g.,* treatment of Ethereum gas, royalties, interest rates, exclusion of zero-value/self-transfers, and documented handling of gifts/OTC transfers) can be applied identically to all class members. This data can be used as a common input to a class-wide damages model consistent with Plaintiff's liability theories that might account for additional factors.

4.5 Opinion 5: Class members can be notified through the blockchain

To the extent that contact information for Metacard NFT holders cannot be ascertained through records, the blockchain can be used as a supplementary notification mechanism for class members. This is a complimentary mechanism to traditional notices through media, press, and advertisements, and other vehicles proposed by Plaintiff. Etherscan provides a user interface for sending private messages to an Ethereum address and the Ethereum addresses of all proposed class members have been determined from blockchain records in the reconstructions in this report. A second approach could send a special-purpose notice token to each address, in an unsolicited fashion which is possible in Ethereum (and referred to as an 'airdrop') with a URL (link) to the notification text. An example of a notice token is located at `0xdc...25f4`, which was ordered for notification purposes by the Supreme Court

of New York in a 2022 case.[17]

5 Declaration

The opinions expressed in this report are based on my review and analysis of the documents I cite. I reserve the right to supplement my report and analysis based on any new evidence brought to my attention. I am over the age of 21. I am competent to make this declaration and I am signing it under the penalty of perjury.

November 13, 2025

Montreal, QC, Canada

References

[1] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. Kroll, and E. Felten. Bitcoin and second-generation cryptocurrencies. In *IEEE Symposium on Security and Privacy*, 2015.

[2] J. Clark and A. Essex. Commitcoin: Carbon dating commitments with bitcoin. In *Financial Cryptography*, 2012.

[3] D. Grandjean. Clustering ethereum addresses. Technical report, ETH Zürich, 2022.

[4] A. Narayanan and J. Clark. Bitcoin's academic pedigree. *Communications of the ACM*, 60(12), 2017.

[17] LCX AG v. John Doe Nos. 1–25, Index No. 154644/2022, NYSCEF Doc. No. 15 (N.Y. Sup. Ct. June 2, 2022) (Order to Show Cause & Temporary Restraining Order) (Masley, J.)

6 Curriculum Vitae

Attached.

September 1, 2025
A more recent version may be available here:
https://www.pulpspy.com/cv/cv.pdf

Jeremy Clark

Associate Professor
Concordia Institute for Information Systems Engineering (CIISE)
Concordia University

j.clark@concordia.ca
+1 (514) 848-2424 x5381
https://pulpspy.com

Table of Contents

Employment

Academic Positions

- Associate Professor, Concordia Institute for Information Systems Engineering (CIISE), Concordia University. 1 June 2018 – present.
- Assistant Professor, Concordia Institute for Information Systems Engineering (CIISE), Concordia University. 1 August 2013 – 31 May 2018.

Professional Designations

- Professional Engineer (non-practicing status). Professional Engineers of Ontario (PEO). December 2018 — present.

Consulting

- Subject matter expert on digital assets, *Scott + Scott Attorneys at Law LLP,* In Re Ethereummax Investor Litigation, 2:22-cv-00163, (C.D. Cal.). Feb 2025—present.
- Subject matter expert on digital assets, *Susman Godfrey LLP,* In re Ripple Labs Inc. Litigation, 4:18-cv-06753, (N.D. Cal.). November 2022—present.
- Subject matter expert on undisclosed cryptocurrency subject, *Williams & Connolly LLP*. January 2018—March 2018.
- Subject matter expert on internet voting security, *City of Toronto*, RFP 3405-13-3197. November 2014—September 2015.

Advisory Boards

- Program Advisory Committee (Information Technology – Cybersecurity/Cybersecurity & Threat Management), Seneca Polytechnic, Oct 2024—present.
- 3iQ Digital Asset Management, Advisory Board, 2017—2021.

Leaves

- Sabbatical: 1 July 2020—30 June 2021
- Parental: 27 October 2019—26 April 2020

Academic Background

Degrees

- Ph.D., Computer Science, University of Waterloo. Graduated: June 2011. Supervisor: Urs Hengartner.
- M.A.Sc., Electrical Engineering, University of Ottawa. Graduated: October 2007. Supervisor: Carlisle Adams.
- B.E.Sc., Computer Engineering, University of Western Ontario. Graduated: April 2004.

Post-Doctorate

- Post Doctoral Fellow, School of Computer Science, Carleton University. 1 July 2011 – 1 August 2013. Supervisor: Paul C. van Oorschot.

Awards

- Excellence in Teaching Award, Junior Faculty Member. Concordia University, 2017.
- Postdoctoral Fellowships Program (PDF). Natural Sciences and Engineering Research Council of Canada (NSERC). 2011–2013
- Alumni Gold Medal (Top Graduating PhD Student). University of Waterloo. 2011
- Alexander Graham Bell Canada Graduate Scholarship (CGS). Natural Sciences and Engineering Research Council of Canada (NSERC). 2008–2011
- David R. Cheriton Graduate Scholarship. University of Waterloo. 2008–2011
- President's Graduate Scholarship. University of Waterloo. 2008–2011
- Grand Prize: Best Election System. "The Punchscan Voting System." University Voting Systems Competition (VoComp). 2007

Publications

Summary

Unlike other fields, the most active venues for security research are **refereed conferences**, as opposed to refereed journals. Given the competitive nature of the top tier conferences, mid-tier venues are often called **workshops**. Unlike in other fields, these are also rigorously peer reviewed venues for completed technical papers and are typically competitive. In our field, the term workshop denotes a venue that is specific to a narrow domain, as opposed to conferences and symposiums, which tend to accept a broad range of papers.

As one illustrative example, our well-publicized work on the Scantegrity voting system (see media below) appeared initially at a **workshop** (USENIX EVT/WOTE which is co-located with USENIX Security; a top-4 and A*). The following year, we published a fuller version of the paper in a **journal** (IEEE Transactions on Information Forensics and Security). The workshop version has been cited 250+ times, while the journal version has been cited only 130+ times.

Statistics

Type	Lifetime	Concordia
Journals & Periodicals	11	9
Refereed Conferences & Workshops	50	30
Book Chapters	5	2

Citations, h-index and i10 index is based on Google Scholar. Google Scholar is automated and not necessarily fully accurate; however it gives representative results.

Updated Fall 2024	Lifetime
Citations	10027
h-index	30

Abbreviations

**Supervised student* *AR = Acceptance rate* *Rank = Core2021*

LNCS XXXX = Volume XXXX of Springer's Lecture Notes in Computer Science

Refereed conference publications

C54	D. Chaum, R.T. Carback, J. Clark, C. Liu, M. Nejadgholi*, B. Preneel, A.T. Sherman, M. Yaksetig, F. Zagorski, B. Zhang. Revisiting Silent Coercion. *Tenth International Joint Conference on Electronic Voting (E-VOTE-ID)*, 2025.
C53	R. Rahimian*, J. Clark. LeverEdge: On-chain leveraged tokens. Fintech & Financial Institutions Conference, 2025.
C52	J. Al-Chami, J Clark. Quest Love: A first look at blockchain loyalty programs. *FinTeachIn, Proceedings of Financial Cryptography and Data Security: FC Workshops,* 2025.
C51	R. Rahimian*, J. Clark. LeverEdge: On-chain leveraged tokens. *Fintech & Financial Institutions Conference*, 2025.
C50	R. Rahimian*, J. Clark. A Shortfall in Investor Expectations of Leveraged Tokens. *Advances in Financial Technology*, 2024.
C49	M. Moosavi*, M. Salehi*, D. Goldman, J. Clark. Fast and Furious Withdrawals from Optimistic Rollups. *Advances in Financial Technology*, 2023.
C48	A. Arun, J. Bonneau, J. Clark. Short-lived zero-knowledge proofs and signatures. *28th Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT)*, 2022. [Rank: A]
C47	D. Demirag*, M. Namazi, E. Ayday, J. Clark. Privacy-Preserving Link Prediction. *17th DPM International Workshop on Data Privacy Management*, 2022.
C46	D. Chaum, R.T. Carback, J. Clark, C. Liu, M. Nejadgholi*, B. Preneel, A.T. Sherman, M. Yaksetig, F. Zagorski, B. Zhang. VoteXX: A Solution to Improper Influence in Voter-Verifiable Elections. *Seventh International Joint Conference on Electronic Voting (E-VOTE-ID)*, 2022.
C45	M. Salehi*, J. Clark, M. Mannan. Not so immutable: Upgradeability of Smart Contracts on Ethereum. *WTSC*, *Proceedings of Financial Cryptography and Data Security: FC Workshops,* 2022.
C44	M. Moosavi*, J. Clark. Lissy: Experimenting with on-chain order books. *WTSC*, *Proceedings of Financial Cryptography and Data Security: FC Workshops,* 2022.
C43	D. Demirag*, J. Clark. Opening sentences in academic writing: How security researchers defeat the blinking cursor. *ACM Technical Symposium on Computer Science Education (SIGCSE TS)*, 2022. [Rank: A]
C42	S. Eskandari*, M. Salehi*, W. C. Gu, J. Clark. SoK: Oracles from the Ground Truth to Market Manipulation. *ACM Advances in Financial Technology*, 2021
C41	M. Salehi*, J. Clark, M. Mannan. Red-Black Coins. *DeFi*, *Proceedings of Financial Cryptography and Data Security: FC Workshops,* 2021.
C40	D. Demirag*, J. Clark. Absentia: secure function evaluation on Ethereum. *WTSC*, *Proceedings of Financial Cryptography and Data Security: FC Workshops,* 2021.

C39	M. Nejadgholi*, N. Yang*, J. Clark. Ballot secrecy for liquid democracy. *VOTING*, *Proceedings of Financial Cryptography and Data Security: FC Workshops,* 2021.
C38	J. Clark, P.C. van Oorschot, S. Ruoti, K. Seamons, D. Zappala. Securing Email. *Proceedings of Financial Cryptography and Data Security (FC),* 2021. [Rank: A]
C37	M Rahimian*, S Eskandari*, J. Clark. Resolving the Multiple Withdrawal Attack in ERC20 Tokens. *2019 IEEE Workshop on Security & Blockchains (IEEE S&B)*.
C36	E. Mangipudi, K. Rao, J. Clark, A. Kate. Automated Penalization of Data Leakage using Crypto-augmented Smart Contracts. *2019 IEEE Workshop on Security & Blockchains (IEEE S&B)*.
C35	S. Eskandari*, M. Moosavi*, J. Clark. Transparent Dishonesty: front-running attacks on Blockchain. *Trusted Smart Contracts*, *Proceedings of Financial Cryptography and Data Security: FC Workshops*, 2019. LNCS 11599.
C34	M. Elsheikh, J. Clark, A. Youssef. Deploying PayWord on Ethereum. *Trusted Smart Contracts*, *Proceedings of Financial Cryptography and Data Security: FC Workshops*, 2019. LNCS 11599.
C33	V. Zhao, J. Choi, D. Demirag*, M. Mannan, K. Butler, E. Ayday, J. Clark. One-time programs made practical. *Proceedings of Financial Cryptography and Data Security (FC)*, 2019. LNCS 11598. [Rank: A]
C32	S. Eskandari*, A. Leoutsarakosg, T. Mursch, J. Clark. A first look a browser-based cryptojacking. *2018 IEEE Workshop on Security & Blockchains (IEEE S&B)*.
C31	C. Okoye*, J. Clark. Toward Cryptocurrency Lending. *Trusted Smart Contracts*, *Proceedings of Financial Cryptography and Data Security: FC Workshops*, 2018. LNCS 10958.
C30	M. Moosavi*, J. Clark. Ghazal: toward truly authoritative web certificates using Ethereum. *Trusted Smart Contracts*, *Proceedings of Financial Cryptography and Data Security: FC Workshops*, 2018. LNCS 10958.
C29	S. Eskandari*, J. Clark, M. Adham, V. Sundaresan. On the feasibility of decentralized derivatives markets. *Trusted Smart Contracts*, *Proceedings of Financial Cryptography and Data Security: FC Workshops*, 2017. LNCS 10323.
C28	N. Yang* and J. Clark. Practical Governmental Voting with Unconditional Integrity and Privacy. *VOTING*, *Proceedings of Financial Cryptography and Data Security: FC Workshops,* 2017. LNCS 10323.
C27	S. Eskandari*, J. Clark, A. Hamou-Lhadj. “Buy your Coffee with Bitcoin: Real-World Deployment of a Bitcoin Point of Sale Terminal.” *Proceedings of the 13th IEEE International Conference on Advanced and Trusted Computing (Bitcoin Track),* 2016.
C26	G. Dagher*, B. Bünz, J. Bonneau, J. Clark, D. Boneh. Provisions: Privacy-preserving proofs of solvency for Bitcoin exchanges. *Proceedings of the 22nd ACM Conference on Computer and Communications Security (CCS)*, 2015. [Rank: A+] AR: 19%

C25	J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. Kroll, E. W. Felten. Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. *Proceedings of the 34th IEEE Symposium on Security and Privacy (IEEE SSP)*, 2015. [Rank: A+] AR: 14%. 3rd highest cited security paper from 2015
C24	S. Eskandari*, D. Barrera, E. Stobert, J. Clark. A First Look at the Usability of Bitcoin Key Management. *Proceedings of the NDSS Workshop on Usable Security (USEC)*, 2015.
C23	D. Barrera, D. McCarney, J. Clark, P. C. van Oorschot. Baton: Certificate Agility for Android's Decentralized Signing Infrastructure. *Proceedings of the 7th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2014.
C22	J. Bonneau, J. Clark, E. W. Felten, J A. Kroll, A. Miller, A. Narayanan. On Decentralizing Prediction Markets and Order Books. *Proceedings of the 13th Annual Workshop on the Economic of Information Security (WEIS)*, 2014.
C21	M. Backes, J. Clark, P. Druschel, A. Kate, M. Simeonovski. Back-Ref: Accountability in Anonymous Communication Networks. *Proceedings of the 12th International Conference on Applied Cryptography and Network Security (ACNS)*, 2014. LNCS 8479. AR: 22%.
C20	J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, E. W. Felten. Mixcoin: Anonymity for Bitcoin with Accountable Mixes. *Proceedings of the 18th Conference on Financial Cryptography and Data Security (FC)*, 2014. LNCS 8437. [Rank: A] AR: 22%
C19	F. Zagorski, R. Carback, D. Chaum, J. Clark, A. Essex, P. Vora. Remotegrity: Design and Use of an End-to-End Verifiable Remote Voting System. *Proceedings of the 11th International Conference on Applied Cryptography and Network Security (ACNS)*, 2013. AR: 23%.
C18	J. Clark and P. C. van Oorschot. SSL and HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements. *Proceedings of the 34th IEEE Symposium on Security and Privacy (IEEE SSP)*, 2013. [Rank: A+] AR: 12%.
C17	D. McCarney, D. Barrera, J. Clark, S. Chiasson, and P. C. van Oorschot. Tapas: Design, implementation, and usability evaluation of a password manager. *Proceedings of the 2012 Annual Computer Security Applications Conference (ACSAC)*, 2012. AR: 19%.
C16	D. Barrera, J. Clark, D. McCarney, P. C. van Oorschot. Understanding and improving app installation security mechanisms through empirical analysis of Android. *Proceedings of the 2nd Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)*, 2012. AR: 37%.
C15	A. Essex, J. Clark, and U. Hengartner. Cobra: Toward concurrent ballot authorization for internet voting. *Proceedings of the 2012 USENIX Electronic Voting Technology Workshop/ Workshop on Trustworthy Elections (EVT/WOTE)*, 2012. AR: 35%.
C14	J. Clark and A. Essex. CommitCoin: Carbon dating commitments with Bit- coin. *Proceedings of the 16th Conference on Financial Cryptography and Data Security (FC)*, 2012. LNCS 7397. [Rank: A]
C13	J. Clark and U. Hengartner. Selections: an internet voting system with over-the- shoulder coercion-resistance. *Proceedings of the 15th Conference on Financial Cryptography and Data Security (FC)*, 2011. LNCS 7035. [Rank: A]

C12	R. Carback, D. Chaum, J. Clark, J. Conway, A. Essex, P. S. Herrnson, T. Mayberry, S. Popoveniuc, R. L. Rivest, E. Shen, A. T. Sherman, P. L. Vora. Scantegrity II Municipal Election at Takoma Park: The First E2E Binding Governmental Election with Ballot Privacy. *Proceedings of the 19th USENIX Security Symposium, 2010*. [Rank: A+] AR: 15%.
C11	A. Essex, J. Clark, U. Hengartner, C. Adams. Eperio: Mitigating Technical Complexity in Cryptographic Election Verification. *Proceedings of the 2010 USENIX Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE)*, 2010.
C10	J. Clark, U. Hengartner. On the Use of Financial Data as a Random Beacon. *Proceedings of the 2010 USENIX Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE)*, 2010.
C09	A. T. Sherman, R. Carback, D. Chaum, J. Clark, A. Essex, P. S. Herrnson, T. Mayberry, S. Popoveniuc, R. L. Rivest, E. Shen, B. Sinha, P. L. Vora. Scantegrity Mock Election at Takoma Park. *Proceedings of the 4th International Conference on Electronic Voting (EVOTE)*, 2010.
C08	J. Clark, U. Hengartner, K. Larson. Not-So Hidden Information: Optimal Contracts for Undue Influence in E2E Voting Systems. *Proceedings of the Second IAVoSS International Conference on E-voting and Identity (Vote-ID)*, 2009, LNCS 5767.
C07	A. Essex, J. Clark, U. Hengartner, C. Adams. How to Print a Secret. *Proceedings of the 4th USENIX Workshop on Hot Topics in Security (HotSec)*, 2009. AR: 28%.
C06	D. Chaum, R. Carback, J. Clark, A. Essex, S. Popoveniuc, R. L. Rivest, P. Y. A. Ryan, E. Shen A. T. Sherman. Scantegrity II: End-to-end verifiability for optical scan election systems using invisible ink confirmation codes. *Proceedings of the 2008 USENIX Electronic Voting Technology Workshop (EVT)*, 2008.
C05	J. Clark, U. Hengartner. Panic passwords: Authenticating under duress. Proceedings of the 3rd USENIX Workshop on Hot Topics in Security (HotSec), 2008. AR: 32%.
C04	A. Essex, J. Clark, C. Adams. Aperio: High integrity elections for developing countries. *Proceedings of the IAVoSS Workshop on Trustworthy Elections (WOTE)*, 2008.
C03	J. Clark, P.C. van Oorschot, C. Adams. Usability of anonymous web browsing: An examination of Tor interfaces and deployability. *Proceedings of the Third Symposium On Usable Privacy and Security (SOUPS)*. ACM International Conference Proceedings Series, vol 229, 2007, pp. 41–51. AR: 31%.
C02	J. Clark, A. Essex, C. Adams. On the security of ballot receipts in E2E voting systems. *Proceedings of the IAVoSS Workshop on Trustworthy Elections (WOTE), 2007*.
C01	A. Essex, J. Clark, R. T. Carback III, S. Popoveniuc. Punchscan in practice: An E2E election case study. *Proceedings of the IAVoSS Workshop on Trustworthy Elections (WOTE)*, 2007.

Articles in journals & periodicals

**Supervised student*

JIF = 2021 Journal Impact Factor, Journal Citation Reports, Web of Science / Clarivate

J11	E.V. Mangipudi, K. Rao, J. Clark, A. Kate. Pepal: Penalizing multimedia breaches and partial leakages. *International Journal of Information Security*, September 2023.
J10	Raphael Auer, Rainer Böhme, Jeremy Clark, Didem Demirag*. Mapping the Privacy Landscape for Central Bank Digital Currencies. *Communications of the ACM*. 66(3):46-53. March 2023. [JIF: 14.065]
J09	E. Pimentel, E. Boulianne, S. Eskandari,* J. Clark. Systemizing the Challenges of Auditing Blockchain-Based Assets. *Journal of Information Systems*, Summer 2021.
J08	J. Clark, D. Demirag*, S. Moosavi*. Demystifying Stablecoins. *Communications of the ACM*. 63(7):40-46. July 2020. [JIF: 14.065]
J07	S. Ruoti, B. Kaiser, A. Yerukhimovich, J. Clark, R. Cunningham. Blockchain Technology: What is it good for? *Communications of the ACM*. 63(1):46-53. January 2020. [JIF: 14.065]
J06	G. Dagher*, B. Fung, N. Mohammad, J. Clark. SecDM: Privacy-preserving Data Outsourcing Framework with Differential Privacy. *Knowledge and Information Systems.* 62:1923–1960, 2020.
J05	A. Narayanan, J. Clark. Bitcoin's Academic Pedigree. *Communications of the ACM*. 60(12):36-45. 2017. [JIF: 14.065]
J04	E. Moher, J. Clark, A. Essex. Diffusion of voter responsibility: potential failings in E2E receipt checking. *USENIX Journal of Election Technology and Systems*. 3(1):1-17. 2014.
J03	J. Clark. Enhancing Anonymity: Cryptographic and statistical approaches for shredding our digital dossiers. *ACM Computing Reviews,* 2014. Invited.
J02	D. Chaum, R. Carback, J. Clark, A. Essex, S. Popoveniuc, R. L. Rivest, P. Y. A. Ryan, E. Shen, A. T. Sherman, P. L. Vora. Scantegrity II: End-to-End Verifiability by Voters of Optical Scan Elections Through Confirmation Codes. *IEEE Transactions on Information Forensics and Security*, 4(4):611-627, 2009. [JIF: 7.231]
J01	D. Chaum, A. Essex, R. T. Carback III, J. Clark, S. Popoveniuc and A. T. Sherman, P. Vora. Scantegrity: end-to-end voter verifiable optical-scan voting. *IEEE Security & Privacy*, vol. 6, no. 3, pp. 40–46, May/June 2008. [JIF: 3.105]

Working papers & technical reports

W04	R. Auer, R. Böhme, J. Clark, D. Demirag. Privacy-enhancing technologies for digital payments: mapping the landscape. *BIS Working Papers*, 1242, 2025.
W03	R. Rahimian*, J. Clark. TokenHook: Secure ERC-20 smart contract, *arXiv*, 2107.02997, 2021.
W02	Y. Nasser, C. Okoye*, J. Clark, P.Y. Ryan. Blockchains and voting: somewhere between hype and a panacea, 2016.
W01	J. Bonneau, J. Clark, S. Goldfeder. On Bitcoin as a public randomness source, *IACR ePrint*, 2015/1015, 2015.

Book chapters

B05	J. Clark. The Long Road to Bitcoin. Foreword to: “Bitcoin and Cryptocurrency Technologies.” *Princeton University Press*, 2016.
B04	R. Carback, D. Chaum, J. Clark, J. Conway, A. Essex, P. S. Herrnson, T. Mayberry, S. Popoveniuc, R. L. Rivest, E. Shen, A. T. Sherman, P. L. Vora. The Scantegrity Voting System and its Use in the Takoma Park Elections. Chapter 10 in: “Real-World Electronic Voting: Design, Analysis and Deployment.” *CRC Press*, 2016.
B03	S. Popoveniuc, J. Clark, R. Carback, A. Essex, D. Chaum. Securing Optical-Scan Voting. Chapter in: “Toward Trustworthy Elections: New Directions in Electronic Voting.” State of the Art Survey Series, *Springer*, 357–369. 2010.
B02	A. Essex, J. Clark, C. Adams. Aperio: High Integrity Elections for Developing Countries. Chapter in: “Toward Trustworthy Elections: New Directions in Electronic Voting.” State of the Art Survey Series, *Springer*, 388–401. 2010.
B01	J. Clark, P. Gauvin, C. Adams. Exit Node Repudiation for Anonymity Networks. Chapter 22 in: “Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society.” *Oxford University Press*. 399-415, 2009.

Editorial activities

E04	J. Clark, E. Shi (Editors). “Financial Cryptography and Data Security: 28th International Conference, FC 2024, Willemstad, Curaçao, March 4–8, 2024, Revised Selected Papers.” Lecture Notes in Computer Science (LNCS) 14744 and 14745. *Springer*, 2025.
E03	Bracciali, A., Clark, J., Pintore, F., Roenne, P., Sala, M. (Editors). “Financial Cryptography and Data Security: FC Workshops 2019.” Lecture Notes in Computer Science (LNCS) 11599. *Springer*, 2020.
E02	A. Zohar, I. Eyal, V. Teague, J. Clark, A. Bracciali, F. Pintore, M. Sala (Editors). “Financial Cryptography and Data Security: FC Workshops 2018.” Lecture Notes in Computer Science (LNCS) 10958. *Springer*, 2019.
E01	J. Clark, S. Meiklejohn, P.Y.A.Ryan, D. Wallach, M. Brenner, K. Rohloff (Editors). “Financial Cryptography and Data Security: FC Workshops 2016.” Lecture Notes in Computer Science (LNCS) 9604. *Springer*, 2016.

Funding

External Funding

Year	Title, Program, Agency	Amount	PI	Co-Applicants
2023	“Understanding Blockchains through Experimentation,” Extension to previous project, Autorité des marchés financiers (AMF)	$200,000 over 3 years Share: 50%	Y	Emilio Boulianne (JMSB)
2021	“Privacy Design Landscape for Central Bank Digital Currencies,” Contributions Program, Office of the Privacy Commissioner of Canada (OPC)	$26,450 once Share: 100%	Y	
2021	“Understanding Blockchains through Experimentation,” Extension to previous project, Autorité des marchés financiers (AMF)	$100,000 once Share: 50%	Y	Emilio Boulianne (JMSB)
2021	“Enhancing transparency, inclusion, and privacy for financial and democratic technologies,” Discovery Grant (DG), Natural Sciences and Engineering Research Council of Canada (NSERC)	$35,000/year for 5 years Share: 100%	Y	
2020	“Toward Scalable Systems for Securities on Blockchains,” Fintech Chaire, Autorité des marchés financiers (AMF) and Finance Montreal	$50,000 once Share: 50%	N	Kaiwen Zhang (ETS)
2019	“NSERC / Raymond Chabot Grant Thornton / Catallaxy Industrial Research Chair on Blockchain Technologies,” Natural Sciences and Engineering Research Council of Canada (NSERC)	$1,380,000 over 5 years Share: 100%	Y	
2017	“Understanding Blockchains through Experimentation,” Education and Good Governance Fund (EGGF), Autorité des marchés financiers (AMF)	$100,000/year for 2 years Share: 50%	Y	Emilio Boulianne (JMSB)
2016	“One Person, One Vote? Blockchain Technologies and Experiments in Voting and Party Governance,” Seed Grant, Centre for the Study of Democratic Citizenship (CSDC)	$6831 once Share: 50%	N	Fenwick Mckelvey (Comm)
2015	“Certificate Authority Report Card: Examining the Root of Data Protection on the Web,” Contributions Program, Office of the Privacy Commissioner of Canada (OPC)	$50,000/year for 1 year Share: 50%	Y	Mohammad Mannan (CIISE)
2015	“Vote par Internet : des technologies favorisant la démocratie,” Programme Établissement de nouveaux chercheurs universitaires, Fonds de recherche du Québec - Nature et technologies (FRQNT)	$19,000/year for 2 years Share: 100%	Y	

Year	Title, Program, Agency	Amount	PI	Co-Applicants
2014	“Secure online services for private user data,” Discovery Grant (DG), Natural Sciences and Engineering Research Council of Canada (NSERC)	$24,000/year for 5 years Share: 100%	Y	

Research Centres (as co-PI)

Year	Title, Program, Agency	Amount	PI	Co-Applicants
2024	“Centre pour l'étude de la citoyenneté démocratique (CECD),” Regroupements stratégiques / Centre en fonctionnement, Fonds de recherche du Québec - Société et culture (FRQSC)	$2,219,922 over 5 years Share: TBD	N	Frédérick Bastien + 46 others
2020	“The Human-Centric Cybersecurity Partnership (HC2P),” Partnership Grant, Social Sciences and Humanities Research Council (SSHRC)	$2,434,323 over 5 years Share: TBD	N	Benoit Dupont + 32 others

Internal Funding

Year	Program	Amount	PI	Co-Applicants
2023	Aid to Research Related Events, Exhibition, Publication and Dissemination Activities (ARRE) Program	$5K once	Y	
2020	Aid to Research Related Events, Exhibition, Publication and Dissemination Activities (ARRE) Program	$5K once	Y	
2015	Aid to Research Related Events, Exhibition, Publication and Dissemination Activities (ARRE) Program	$5K once	Y	
2015	Individual Seed Program	$7K once	Y	
2013	Start-Up Grant	$50K once	Y	

Research Centres Membership

- Human-Centric Cybersecurity Partnership (HC2P). Co-Investigator, 2020—present.
- Centre for the Study of Democratic Citizenship (CSDC). Co-investigator, 2016—present. Advisory board member, 2022—present.
- Smart Cybersecurity Network (SERENE-RISC). Knowledge Mobilization Network, Networks of Centres of Excellence of Canada (NCE). Co-Investigator, 2016—2021.

Evidence of Impact

Invited Talks and Seminars

- a16z crypto, “Towards Succinct Proofs of Solvency,” Invited Talk, June 18, 2024.
- CSNet 2023, "Privacy Options for Central Bank Digital Curriencies (CBDCs)." Keynote, October 17, 2023.
- Cyberjustice Labratory, University of Montreal, "Web3: Landscape and Future Directions." Keynote, October 16, 2023.
- Cybersecurity and Privacy Institute (CPI) Annual Conference, University of Waterloo. "Transparent Dishonesty: front-running attacks on Blockchain." Invited Talk, October 12, 2023.
- UMBC Cyber Defense Lab Seminar, "Fast Withdrawals from Optimistic Rollups.” Invited Talk, September 8, 2021.
- a16z crypto, “Fast Withdrawals from Optimistic Rollups,” Invited Talk, June 27, 2023.
- MIT Digital Currency Initiative (DCI), “Privacy Options for Central Bank Digital Curriencies (CBDCs),” May 23, 2023.
- Berkman-Klein Center for Internet & Society (Harvard), “Privacy Options for Central Bank Digital Curriencies (CBDCs),” Blockchain and Privacy Workshop, May 22, 2023.
- Digital Economy Taxation Network / Revenu Québec, DET 2023, “Going Digital: Tax Systems and Emerging Technology,” Panel, June 18, 2023.
- C-Dem/CSDC Forum, “Roundtable: Electoral Integrity,” Panel, June 4, 2023.
- CIADI/GCS Aerospace Meets Cybersecurity Forum, “Cybersecurity challenges in aerospace,” Moderator, April 17, 2023.
- Financial Management Institute of Canada, PD Week. "Blockchain and DeFi: Landscape," November 24, 2022.
- FIC, International Cybersecurity Forum, November 1-2, 2022.
- MTL Connect, "MTL Inspire." Panel, October 19, 2022.
- ACT International Midterm Conference, "Policing Blockchain." Panel, October 6, 2022.
- Fintech Cadence | Fintech Drinks, “Fintech & DeFi: How is fintech DeFi-ing the traditional banking system?” Panel, July 12, 2022.
- Blockchain Technology Symposium. “Blockchain Culture, Leisure and Luxury.” Panel, June 10, 2022.
- Quartier de l’innovation de Montréal. “Entre Terre et techno, ça clique ?” Panel, May 26, 2022.
- Fintech Cadence Certificate Program. "Understanding blockchain and its uses in the financial sector.” February 22, 2022.
- Autorité des marchés financiers. “Finance décentralisée et crypto : état de la situation, nouveaux risques et points de vigilance.” Panel, October 26, 2021.
- Smith School of Business, Queen’s University. “New Frontiers in Auditing: Risk and Opportunities in the Blockchain Sector.” Panel, October 7, 2021.

- Vancouver International Privacy & Security Summit (VIPSS). “Banking on the Future: How the Digital Surge Will Reshape How We Do Business.” Panel, May 6, 2021.
- CyberEco Cyber Conference. “Technology & blockchain.” May 5, 2021.
- Quartier de l’innovation de Montréal. “Blockchain - multiples usages.” Panel, April 28, 2021.
- Holt Accelerator, “[I AM PROTECTED].” Panel, April 21, 2021.
- UMBC Cyber Defense Lab Seminar. “Transparent Dishonesty: front-running attacks on Blockchain.” March 26, 2021.
- 1st Annual Lecture on Computer Science and Society. “The Blockchain and Cryptocurrency Landscape.” Carleton University. March 10, 2021
- Workshop on The State of Canadian Cybersecurity Conference: Human-Centric Cybersecurity. “Decentralized Finance: Landscape and Future Directions.” SERENE-RISC, February 18, 2021.
- Fintech Cadence Certificate Program. "Understanding blockchain and its uses in the financial sector.” January 30, 2021.
- Montreal Lakeshore University Women's Club. “Bitcoins: What, why and how…” February 10, 2020.
- Elections Quebec. "Internet Voting." November 2, 2019.
- Blockchain at McGill. “Introduction to Blockchain for Non-Profits,” Social Innovation: Int’l Development and Blockchain. 29 March 2019.
- Canada Mortgage and Housing Corporation (CMHC). "Blockchain Technologies: Landscape and Future Directions.” 26 February 2019.
- CFA Montreal FinTech Rendez-vous. "Blockchain Technologies: Landscape and Future Directions.” 7 February 2019.
- Loto-Quebec. “Lunch and learn.” 22 January 2019.
- RISQ Colloquium. "Blockchain Technologies: Landscape and Future Directions.” 29 November 2018.
- TriPAC Pension Advisory Committees. "Blockchain Technologies: Landscape and Future Directions." Treasury Board Secretariat. 21 November 2018.
- Defending Democracy: Confronting Cyber-Threats At Home And Abroad. "Liquid Democracy and Blockchains." October 26, 2018.
- Blockchain and National Security. "Blockchain Technology: National Security Use-Cases." Public Safety Canada, October 18, 2018.
- Montreal Police Pension Fund (ABRPPVM). “Blockchain Technology: Landscape & Future Directions.” Invited speaker, September 22, 2018.
- BMO 13th Annual Realestate Conference. “Blockchain Applications & Real-Estate.” Panel, BMO Capital Markets. September 20, 2018.
- Blockchain Technology Symposium (BTS). “Blockchain Nuances: Lessons from Fintech use-cases.” Invited talk, Fields Institute. September 18, 2018.
- GoSec. “Blockchain Technologies: Landscape and Future Directions.” August 29, 2018.
- StartupFest. “Democracy Enhancing Technologies.” CryptoFest. July 10, 2018.

- FinteQC. "Blockchain Nuances" Keynote, Desjardins Labs & UQAR, June 20, 2018.
- The Walrus LIVE. "The Future of Money" Panel Discussion with David Tax (TD) and Susan Prince (CBC). June 14, 2018.
- BMO ThinkSeries. "Blockchain Technologies: Landscape and Future Directions." June 12, 2018.
- Autorite des marches financiers (AMF). "Crypto Primer II." June 11, 2018.
- Canada Pension Plan Investment Board (CPPIB). "Blockchain Technologies." June 1, 2018.
- Security Revolution. "Blockchain Primer." SERENE-RISC, May 31, 2018.
- “Blockchain Technologies: Landscape and Future Directions.” True North Science Bootcamp. May 25, 2018.
- Anticipating Future Trends and Managing Risks Program. "Blockchain Technologies: Landscape and Future Directions," HEC Paris and Concordia. May 10, 2018.
- Autorite des marches financiers (AMF). "Crypto Primer I." May 1, 2018.
- GC Blockchain Day. “Ledgers Past, Present and Future.” Treasury Board Secretariat of Canada. April 23, 2018.
- “Workplace 2020.” Management Consulting Club, Concordia. Panel. April 8, 2018.
- “Blockchain Technologies: Landscape and Future Directions.” Canadian National Railway (CN). February 8, 2018.
- Kenneth Woods Portfolio Management Program. “Cryptocurrencies: An Investable Asset?” John Molson School of Business. January 23, 2018.
- "Provisions: Privacy-Preserving Proofs of Solvency." Newcastle University. December 7, 2017.
- "Democracy Enhancing Technologies: From Theory to Practice." CSDC Speaker Series. McGill, September 15, 2017.
- Hydro-Québec Symposium 3i. “Bitcoin & Blockchains: Landscape and Future Directions.” Invited Speaker, Montreal,
- Privacy, Security and Trust (PST). “Bitcoin & Blockchains: Landscape and Future Directions.” Keynote, Calgary, August 28, 2017.
- Metropolis 2017. “The Bitcoin & Blockchain Technology Landscape.” June 28, 2017.
- Blockchain Meetup. “Zero Knowledge.” District 3. May 4, 2017.
- Canada Music Week. “Blockchains: Smart Contracts and Media-Driven Crypto Currencies” Panel discussion, April 19, 2017.
- District 3. “The Future of Blockchain.” Panel discussion, December 8, 2016.
- Symposium on Foundations & Practice of Security. “The Bitcoin & Blockchain Technology Landscape.” Keynote presentation. Université Laval, October 26, 2016.
- Online Voting Roundtable: Electoral Futures in Canada. “Blockchain and Voting: Assessment & Critique.” Invited Speaker, University of Ottawa. September 26, 2016.
- P2P Financial Systems Workshop. “Blockchain nuances.” Keynote presentation. UCL, September 8, 2016.
- Bank of Canada. ”Bitcoin & Blockchains: Part 2.” July 14, 2016.

- Anti-phishing working group (APWG) eCrime 2016. "Bitcoin: an impartial assessment of its use and potential for cybercrime." May 31, 2016.
- C.D. Howe. ”Blockchain Technologies and the Future of Finance." May 30, 2016.
- ASIMM Colloque RSI. "Bitcoin & Blockchains: Tutorial,” May 12, 2016.
- Bank of Canada. ”Bitcoin & Blockchains: Landscape and Future Directions,” May 11, 2016.
- National Research Council (NRC), “Security Training Course,” March 22, 2016.
- MIT Bitcoin Expo. ”Blockchain-based voting: potential and limitations,” MIT, March 6, 2016.
- Bitcoin and Cryptocurrency Research Conference. “Altcoins,” Center for Information Technology Policy (CITP), Princeton University, March 27, 2014.
- USENIX Summit on Hot Topics in Security (HotSec 2013). “Eroding Trust and the CA Debacle,” August 13, 2013.
- CIISE Distinguished Seminar. “How to Carbon Date Digital Information,” Concordia University, March 8, 2012.
- MITACS Digital Security Seminar Series. “Panic Passwords and their Applications,” Carleton University, January 27, 2011.
- CACR Cryptography Seminar. “The First Governmental Election with a Voter Verifiable Tally: Experiences using Scantegrity II at Takoma Park,” University of Waterloo, February 5, 2010.
- CACR Cryptography Seminar. “Selections: An Internet Voting System with Over-the- shoulder Coercion Resistance,” University of Waterloo, December 3, 2010
- Information Technology and Innovation Foundation (ITIF) Forum: Future of Voting. “Panel Discussion,” Longworth House Office Building, Washington, D.C. March 6, 2008.
- CACR Cryptography Seminar. “Combating Adverse Selection in Anonymity Networks,” University of Waterloo, October 17, 2007.

Expert Testimony & Public Interest Consultations

- Elections Quebec. "Internet Voting,” Citizen Jury. November 2, 2019.
- House of Commons, Standing Committee on Finance. Testimony: Statutory Review of the Proceeds of Crime and Terrorist Financing Act. March 27, 2018.
- Investissement Quebec. Bitcoin & Blockchains: Landscape and Future Directions. January 15, 2018.
- Government of Canada (GC) Digital Target State Architecture and Direction. Blockchain working group. August 2017 — April 2018.
- Karina Gould, Minister of Democratic Institutions (House of Commons, Canada). CSDC roundtable. August 30, 2017.
- Autorité des marchés financiers (AMF). “Blockchain nuances.” March 29, 2017.
- Royal Canadian Mounted Police (RCMP). Bitcoin brainstorming session (#2). Participant in roundtable. September 28, 2016.
- Royal Canadian Mounted Police (RCMP). Bitcoin brainstorming session. Participant in roundtable. July 5, 2016.

- Formation régionale de la Cour du Québec. ”Bitcoin: Introduction & Implications,” May 9, 2015.
- 2013–2014 City of Toronto. Subject Matter Expert on Internet Voting Security and Cryptography (RFP No. 3405-13-3197).
- Senate of Canada, Standing Committee on Banking, Trade and Commerce. Testimony: Study on the use of digital currency. April 3, 2014.
- City of Edmonton: Citizen Jury on Internet Voting. “Security Risks Related to Internet Voting,” Centre for Public Involvement/University of Alberta, November 23–25, 2012.

Press & Media (Selected)

- “Where Did Bitcoin Come From?” *Mornings With Sue And Andy. QR Calgary 770*, 8 November 2024.
- “Who Invented Bitcoin?” *Mornings with Simi, CKNW 980*, 4 November 2024.
- “Did a Canadian developer really invent bitcoin? A new HBO show explores an intriguing theory,” *The Conversation*, 31 October 2024.
- “Parsing Satoshi: What the Malmi emails reveal about Bitcoin’s creator,” *CoinTelegraph*, March 6, 2024.
- “Bridging traditional investment with cryptocurrencies? One Canadian miner tried it,” *CBC News,* January 24, 2024.
- “Two years after peak crypto, Bitcoin has faded from the political conversation,” *CBC News*, November 3, 2023.
- “Are Quebec’s Crypto Mines Here to Stay?” *The Rover*, June 16, 2023.
- “What is Worldcoin and what does it mean for our privacy?” *Context.news (Thomson Reuters Foundation)*, June 7, 2023.
- “Clarity, please.” *CBA/ABC National*, November 14, 2022
- “Deception, exploited workers, and cash handouts: How Worldcoin recruited its first half a million test users.” *MIT Technology Review*, April 6, 2022.
- “It's a first, Bitcoin is now legal tender in one country.” *CBC Radio*, September 23, 2021.
- “New kid on the blockchain: the young people using crypto for good.” *DAZED*, July 22, 2021.
- “Digital currencies bring new options for financial privacy.” *Hill Times*, May 5, 2021.
- “Satoshi & Company: The 10 Most Important Scientific White Papers In Development Of Cryptocurrencies.” *Forbes*, February 13, 2021.
- “Contact tracing segment.” *The Aaron Rand Show, CJAD 800*, May 26, 2020.
- “Are we ready for an app that trades privacy for more freedom?” *Montreal Gazette*, May 25, 2020.
- “Chaînes de blocs: dompter la décentralisation de l’informatique.” *Le Devoir*, March 2, 2020.
- “Academic: All Undergrads Should Learn About Bitcoin & Blockchain.” *Cryptonews*, December 22, 2019.
- “Why Quebec is betting big on Bitcoin.” *Pivot Magazine (CPA Canada)*, January 8, 2019.

- "Banks Claim They're Building Blockchains. They're Not." *Investopedia*, July 13, 2018.
- "The evolution of cryptojacking." *CryptoInsider*, March 20, 2018.
- "The Ethics Of Cryptojacking: Rampant Malware Or Ad-Free Internet?" *CoinTelegraph*, March 16, 2018.
- "One of the Biggest Coinhive Users Made $7.69 In 3 Months." *Motherboard*, March 14, 2018.
- "Attack Or Business Opportunity?: Academics Question Ethics Of Coinhive Cryptojacking." *CoinTelegraph*, March 10, 2018.
- "How much should I regret not buying Bitcoin?" Gizmodo, January 29, 2018.
- Interview on Bitcoin regulation. *CBC Radio One,* December 5, 2017.
- "How blockchain-based payment is changing the cannabis industry," *IBM thinkLeaders*, June 21, 2017.
- "Ottawa explores potential of 'blockchain,' billed as next-generation Internet tech." *Toronto Star*, February 28, 2017.
- "Block the vote: Could Blockchain Technology Cybersecure Elections?" *Forbes*, August 30, 2016.
- "He's Bitcoin's Creator, He Says, but Skeptics Pounce on His Claim," *New York Times*, May 2, 2016.
- "Logged out, but still out there," *Globe and Mail*, February 19, 2016.
- "Princeton University releases first draft of bitcoin textbook," *CoinDesk*, February 10, 2016.
- "The top 10 cryptocurrency research papers of 2015," *CoinDesk*, December 27, 2015.
- "Canada's Internet Voting Problem," *SC Magazine*, February 2015 issue.
- "Latest Internet voting reports show failures across the board," *Al Jazeera America*, February 8, 2015
- "How Block Chain Technology Could Usher in Digital Democracy," *CoinDesk*, June 16, 2014.
- "Can Bitcoin Help Predict the Future?," *CoinDesk*, May 24, 2014.
- "Heartbleed and sentinels of the net," *Montreal Gazette*, Apr 21, 2014.
- "PROFESSOR: There Is A Big, Gaping Flaw In The New Satoshi Study," *Business Insider*, March 28, 2014.
- "2014 Federal Budget Calls Bitcoin A Terrorist, Crime 'Risk', " *Huffington Post*, February 12, 2014.
- "Bitcoin: How its core technology will change the world," *New Scientist*, February 5, 2014.
- "More than money, bitcoin's real value lies in its algorithms," *InfoWorld*, January 12, 2014.
- "U. researchers develop Bitcoin prediction market," *Daily Princetonian*, January 5, 2014.
- "This Princeton professor is building a Bitcoin-inspired prediction market," *The Verge*, November 29, 2013
- "Montreal's Bitcoin Embassy bridges gap between digital currency and real world," *Montreal Gazette*, November 29, 2013.

- "Bitcoin online currency gets new job in web security," *New Scientist*, January 11, 2012.
- "Secure, verifiable voting: Cryptography, invisible ink, and other voting magic," *Imprint*, November 6, 2009.
- "Scantegrity: Voters Test New Transparent Voting System," *Huffington Post*, November 5, 2009.
- "Maryland Voters Test New Cryptographic Voting System," *Wired News*, November 4, 2009.
- "Voters try out new security system," *UW Daily Bulletin*, November 3, 2009.
- "E-voting system lets voters verify their ballots are counted," *Computerworld*, November 3, 2009.
- "First Test for Election Cryptography," *Technology Review*, November 2, 2009.
- "Mock election tests new voting system," *Gazette.net*, April 15, 2009.
- "Geek the Vote 2012: What Election Tech Will Look like 4 Years From Now," *Popular Mechanics*, November 4, 2008.
- "Canadian voting machine technology enters American political scene," *CBC.ca*, October 28, 2008.
- "New Voter Counter System Uses Encrypted Codes, Invisible Ink," *Voice of America*, October 24, 2008.
- "A Really Secret Ballot," *The Economist*, October 22, 2008.
- "Class voting hacks prompt call for better audits," *MSNBC*, October 20, 2008.
- "Clean Elections," *Communications of the ACM*, October 2008.
- "Protecting Your Vote With Invisible Ink," *Discover Magazine*, October 2008.
- "Flawless Vote Counts," *Technology Review*, September/October 2008.
- "Shift Back to Paper Ballots Sparks Disagreement," *Morning Edition*, March 7, 2008.
- "Down for the Count," *ACM netWorker*, March 2008.
- "The future of voting IT," *Government Computer News*, March 10, 2008.
- "A Damaging Paper Chase In Voting," *Washington Post*, September 8, 2007.
- "Punchscan Wins VoComp 2007," *As It Happens (CBC)*, August 23, 2007.
- "US/Canada Team Wins Voting Competition," *Threat Level (Wired)*, July 19, 2007.
- "Electronic Democracy," *Digital Planet (BBC)*, January 29, 2007.
- "Making Every E-vote Count," *IEEE Spectrum*, January 2007.

Concordia Promotional Activities

- Thinking Out Loud. "Bitcoin & Cryptocurrency," Podcast, Episode 14. 27 February 2018.
- "Back to the future — reclaiming the internet" Distinguished Alumni Speaker Series with Fay Arjomandi. September 22, 2018.
- This is Concordia. Now. "Bitcoin and cryptocurrency." Conversation with Alan Shepherd. April 11, 2018.

- "X EXPLAINED: What you need to know about internet cookies." Concordia Video. March 29, 2018.
- This Is Concordia. Now. "Jeremy Clark talks Bitcoin and cryptocurrency." Conversation with Sudha Krishnan (CBC Montreal). February 22, 2018.
- Next-Gen. Now. "The Campaign for Concordia." Promotional video with on-screen interview. November 24, 2017.
- Capstone Magazine. "Cyberattacks: everything you need to know." Fall 2016.
- Concordia Alumni Association. "Everyone knows your birthday: How secure is your password Hint: not very!" New York City, May 16, 2017.
- Thinking Out Loud. "One Vote," The Futurecast podcast, Episode 4. April 12, 2017.
- Next-gen. Now. "My Name is Jeremy Clark." Website feature. March 1, 2017.
- Concordia University Magazine. "Guardians of the IT galaxy." February 9, 2017.
- Thinking Out Loud. "Connecting your tech future," conversation with Nora Young (CBC), Concordia University. March 1, 2016.
- Breakfast Talk. "Heartbleed & other CIISE Research," Concordia University. May 6, 2014.

Highly Qualified Personnel

HQP Job Placement

Sector	Organization
Blockchain Industry	ConsenSys Diligence, Offchain Labs, Trail of Bits, Quantstamp, BitAccess, Ether Capital
Faculty	Carleton University, Boise State University
PhD, Post-Doctoral	UQAM
General Industry	KPMG, Deloitte, Morgan Stanley
Government	National Defence

Includes jobs while in program and first job after graduation

Post-Doctoral (Completed)

Name	Dates	Research Topic	Papers	Co-Supervisor
Vathsan Morkonda	2024/W - 2025/W	Usable security		
Elizabeth Stobert	2018/W-2018/F	Usable security	C24	

/F (Fall term), /W (Winter term), /S (Summer term)

PhD (Completed)

Name	Dates	Dissertation Title	Papers	Co-Supervisor
Mahsa Moosavi	2018/S-2025/S	“Navigating decentralized finance (DeFi) risks and challenges through user-centric solutions”	C30, C35, J08, C44, C49	
Reza Rahimian	2018/F-2025/W	“Enhancing DeFi by improving ERC-20 Token Security and Addressing Leveraged Token Shortcomings”	C37, C50, C51, W03	
Shayan Eskandari	2017/F-2024/F	“The Hidden Layers of Blockchains: Technical Nuances and their Unforeseen Consequences”	C24, C27, C29, C32, C35, C37, C42, J09	
Didem Demirag	2018/W-2022/F	“Moving Multiparty Computation Forward for the Real World”	C33, J08, C40, C43, C47, J10	

Name	Dates	Dissertation Title	Papers	Co-Supervisor
Nan Yang	2014/ S-2020/F	“Non-Local Contamination in Cryptography”	C28, C39	C. Crépeau (McGill)
Gaby Dagher	2013/F - 2015/F	“Toward secure and privacy-preserving data sharing and integration”	C26, J06	B. Fung (McGill)

Masters (Completed)

Name	Dates	Thesis Title	Papers	Co-Supervisor
Antoine Cyr	2023/ W-2025/S	“Daily Proofs of Liabilities”		S. Bergler (CSSE)
Youwei Deng	2023/ W-2025/ W	“Xiezhi: Toward Succinct Proofs of Solvency”		
Sina Pilehchiha	2021/ S-2022/F	“Improving Reproducibility in Smart Contract Research”		A.G. Aghdam (ECE)
Mahdi Nejadgholi	2019/ F-2022/S	“Nullification, a coercion-resistance add-on for e-voting protocols”	C39, C46	
Mehdi Salehi	2020/ W-2022/ W	“An Analysis of Upgradeability, Oracles, and Stablecoins in the Ethereum Blockchain”	C41, C42, C45, C49	M. Mannan (CIISE)
Corentin Thomasset	2019/ F-2020/S	“SERENIoT : Politiques de sécurité collaboratives pour maisons connectées”		D. Barrera (Carleton), J. Fernandez (Polytechnique)
Chidinma Okoye	2016/S - 2017/F	“New applications of blockchain technology to voting and lending”	C31, W02	
Mahsa Moosavi	2015/F - 2018/W	“Rethinking Certificate Authorities: Understanding and decentralizing domain validation”	C30, C35, J08, C44, C49	
Michael Colburn	2014/F - 2018/S	“Short-Lived Signatures”		
Abhimanyu Khanna	2014/F - 2017/S	“Towards Usable and Fine-grained Security for HTTPS with Middleboxes”		M. Mannan (CIISE)
Shayan Eskandari	2013/F - 2016/W	“Real world deployability and usability of Bitcoin”	C24, C27, C29, C32, C35, C37, C42, J09	W. Hamou-Lhadj (ECE)

PhD (In Progress)

Name	Dates	Research Topic	Papers	Co-Supervisor
Nahid Rahman	2024/F-	Blockchain analytics		
Pratyusha Bhattacharya	2017/S-	Smart Grid Security		M. Debbabi (CIISE)

Masters (In Progress)

Name	Dates	Research Topic	Papers	Co-Supervisor
Kimia Esmaili	2025/S-	Zero-Knowledge Proofs		
Anton Zhekov	2025/W-	Network Science		P. Miasnikof (Laval)

Supervised Graduate Projects (ENGR 6991)

Year	Students
2025	Adrijeet Deb
2024	Arun Sankar
2023	Mohammad Zawad Tahmeed
2019	Abhinav Kumar
2018	Jinumol James, Laleh Alimadadi, Rupesh Gawde, Brindha Shree, Isreal Tei
2018	Saad Ahmen (MIAE: ENGR 6971)
2017	Temitiope Adetula, Shahab Odagar
2016	Ejiro Mary, Ogor Umukoro, Omoye Obazele
2015	S. Sandisha
2014	Paemka-Ojugbana Judah Chukwuma, Manish Megnath

Teaching

Courses Taught

Year/Term	Course	Class Size	Evaluation
2025 W	INSE 6150: Security Evaluation Methodologies		
2024 F	INSE 6615: Blockchain Technology	88	1.15
2024 F	INSE 6150: Security Evaluation Methodologies	102	1.13
2024 W	INSE 6615: Blockchain Technology	89	1.41
2024 W	INSE 6150: Security Evaluation Methodologies	87	1.46
2023 F	INSE 6150: Security Evaluation Methodologies	118	1.16
2023 W	INSE 6615: Blockchain Technology	69	1.30
2024 W	INSE 6150: Security Evaluation Methodologies	100	1.48
2022 F	INSE 6150: Security Evaluation Methodologies	70	1.72
2022 W	INSE 6630: Recent Developments in Info. Systems Security	67	*Evaluations suspended (COVID)*
2022 W	INSE 6150: Security Evaluation Methodologies	68	
2021 F	INSE 6150: Security Evaluation Methodologies	49	
2020 S1	INSE 6150: Security Evaluation Methodologies	78	
2019 W	INSE 6150: Security Evaluation Methodologies	92	1.20
2019 W	COMP 249: Object Oriented Programming II	109	1.73
2018 F	INSE 6630: Recent Developments in Info. Systems Security	53	1.19
2018 F	COMP 352: Algorithms and Data Structures	68	1.57
2018 W	INSE 6150: Security Evaluation Methodologies	88	1.69
2017 F	INSE 6110: Foundations of Cryptography	79	1.22
2017 F	INSE 6630: Recent Developments in Info. Systems Security	35	1.71
2017 W	INSE 6150: Security Evaluation Methodologies	59	1.13
2016 F	INSE 6150: Security Evaluation Methodologies	63	1.09
2016 F	INSE 6110: Foundations of Cryptography	79	1.32
2016 W	COMP 249: Object Oriented Programming II	50	1.44
2016 W	INSE 6150: Security Evaluation Methodologies	86	1.15

Year/Term	Course	Class Size	Evaluation
2015 F	INSE 6110: Foundations of Cryptography	76	1.24
2015 W	COMP 249: Object Oriented Programming II	93	1.81
2015 W	INSE 6150: Security Evaluation Methodologies	86	1.41
2014 F	INSE 6110: Foundations of Cryptography	69	1.55
2014 W	INSE 6150: Security Evaluation Methodologies	46	1.73
2013 F	INSE 6110: Foundations of Cryptography	21	1.11

- *Evaluation scores are between 1.00 (best) to 5.00 (worst)*
- *2024 F-present: Question 5: "The instructor clearly explains the course content."*
- *2013-2024 W: Question 20: "Overall, the professor is an effective teacher."*

Teaching Awards

- Teaching Excellence Award, Junior Faculty, ENCS, Concordia University, 2017.

External Lectures

- "Decentralized finance (DeFi)," Faculty of Law, University of Ottawa. 22 March 2021.
- "Improving usability and trust for moving Bitcoin adoption forward," MAS.S65 - Blockchain Technologies, Massachusetts Institute of Technology (MIT). Guest lecture, 4 November 2015.
- "History of cryptocurrencies," Bitcoin and Cryptocurrency Technologies, Princeton University. Guest lecture, Online: Coursera, recorded in September 2015.
- COMP 4109: Applied Cryptography, Carleton University. Course, Winter 2013.

Service to University

University Committees

Leaves: Parental 2019-2020; Sabbatical 2020-2021

Year	Committee
2024-	GCS EDI Award and Research Grant Committee
2024-	GCS Faculty Research Committee (FRC)
2023-	GCS Faculty Personnel and Tenure Committee (FPTC)
2023-	CIISE Curriculum Committee
2022-	GCS Elections Committee (Chair)
2021-2023	Concordia University Faculty Tribunal Pool
2021-2023	GCS Faculty Council
	Parental Leave and Sabbatical
2018-2019	Concordia University Faculty Tribunal Pool
2018-2019	ENCS Blended/Online Pedagogy Committee
2017-2019	ENCS Elections Committee
2013-2019	CIISE Seminar Committee
2014–2016	Concordia University Faculty Tribunal Pool

Graduate Student Committees (Concordia)

Year	Occurrences					
	MASc Defence	PhD Comp.	PhD Proposal	PhD Seminar	PhD Defence	Total
2025		1	1		2	4
2024	5	2	1	2	2	12
2023	5	1	2	1		9
2022	1	2	1	3	1	8
2021	3	1	1	1	1	7
2020	4	1		1	1	7
2013-2019	6	9	6	7	7	35

External Examiner

- Bofeng Pan, PhD, University of Saskatchewan, 2024
- Ghassan Al-Sumaidaee, PhD, McGill, 2024
- Alireza Arjmand Shakouri, Masters, University of Alberta, 2023
- Md Mamunur Rashid Akand, PhD, University of Calgary, 2023
- Farimah Ramezan Poursafaei, PhD, McGill, 2022
- Patrick McCorry, PhD, Newcastle University, UK, 2017
- Giulia Alberini, PhD, McGill, 2015
- Jérôme Dossogne, PhD, Université libre de Bruxelles, Belgium, 2015

Service to Academia

Program (Co-)Chair (Conferences)

Year	Conference
2024	Financial Cryptography and Data Security 2024 (FC)
2022	Blockchain Technology Symposium (BTS)
2019	FC Workshop on Advances in Secure Electronic Voting (VOTING)
2018	FC Workshop on Advances in Secure Electronic Voting (VOTING)
2017	The Smart Cybersecurity Network: Spring 2017 Workshop (SERENE-RISC)
2016	FC Workshop on Bitcoin and Blockchain Research (BITCOIN)

General (Co-)Chair (Conferences)

Year	Conference
2024	Blockchain Technology Symposium (BTS)
2023	Blockchain Technology Symposium (BTS)
2020	Privacy Enhancing Technologies Symposium (PETS)

Advisory/Editorial Boards (Conferences/Journals)

Year	Journal
2019—2024	Privacy Enhancing Technologies Symposium (PETS)
2013—2015	USENIX Journal of Election Technologies (USENIX JETS)

Program Committees (Conferences)

Year(s)	Conference
2023—	ACM Computer and Communications Security (CCS): Blockchain Track
2025—	USENIX Security Symposium
2016—	Financial Cryptography and Data Security (FC)
2023—	Advances in Financial Technology (AFT)
2021—	International Joint Conference on Electronic Voting (E-VOTE-ID)

Year(s)	Conference
2021—	ACM CCS Workshop on Decentralized Finance and Security (DeFiSec)
2023—	Science of Blockchain Conference (SBC)
2025—	The Latest in DeFi Research (tldr)
2017—2024	ESORICS Workshop on Cryptocurrencies and Blockchain Technology (CBT)
2022—2024	FC Workshop on Decentralized Finance (DeFi)
2022	Workshop on Privacy in the Electronic Society (WPES)
2018—2021	IEEE Security & Privacy on the Blockchain (IEEE S&B)
2013—2018	FC Workshop on Bitcoin Research (BITCOIN)
2017—2018	APWG Symposium on Electronic Crime Research (eCrime)
2018	Symposium on Usable Privacy & Security (SOUPS)
2016	RSA Conference: Cryptographer's Track (CT-RSA)
2016	ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)
2014	Annual Computer Security Applications Conference (ACSAC)

Reviewer: Journals (Most Recent Year)

Most Recent Year	Journal / Conference
2024	IEEE Transactions on Network and Service Management (TNSM)
2024	IEEE Transactions on Parallel and Distributed Systems (TPDS)
2024	IEEE Transactions on Network Science and Engineering (TNSE)
2023	IEEE Security and Privacy Magazine (S&P)
2022	IEEE Transactions on Information Forensics and Security (TIFS)
2021	Bank for International Settlements Working Paper Series (BIS WPS)
2021	IEEE Transactions on Dependable Secure Computing (TDSC)
2021	Communications of the ACM (CACM)

Reviewer: Funding Agencies (Most Recent Year)

Most Recent Year	Agency
2025	Natural Sciences and Engineering Research Council of Canada (NSERC)
2024	Social Sciences and Humanities Research Council of Canada (SSHRC)
2024	MITACS
2024	National Cybersecurity Consortium (NCC)
2024	Austrian Science Fund (FWF)
2023	Israel Science Foundation (ISF)
2023	Luxembourg National Research Fund (FNR)
2019	Fonds de Recherche du Québec – Nature et technologies (FRQNT)
2019	Alberta Innovates
2017	Office of the Privacy Commissioner of Canada (OPC)

Reviewer: Prizes (Most Recent Year)

Most Recent Year	Agency
2024	Bitcoin Research Prize, Chaincode Labs